RCMP
ROYAL CANADIAN MOUNTED POLICE

Serving the police community since 1938

GAZETTE

Vol. 70, No. 3, 2008
www.rcmp-grc.gc.ca

On the Watch

Approaching national security from the inside out

Domestic terrorism
RCMP tackles the threat from within

Web-savvy ways
U.S. intelligence community embraces Web 2.0

Tired cops
Managing police fatigue

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

On guard for national security

A terrorist bomb. Web-based terror tactics. A high-level security breach. A major financial fraud. These are but a few of the scenarios that can have a direct and serious impact on national security.

In this issue, we look at how law enforcement agencies are arming themselves with the knowledge and skills to prevent and prepare for such incidents, and respond effectively when they do occur.

In our cover article, writer Caroline Ross looks at the increasing threat from domestic extremists in Canada — and the RCMP's role in investigating cases with possible terrorist links. Read about what it takes to build top-quality investigations when it comes to suspicious terrorist activities.

Preparing for a national security incident is a complex task in today's borderless world. The *Gazette* was on hand to observe a day-long emergency response exercise involving three simultaneous attacks in Hamilton, Ontario. Find out how the more than 100 first responders from numerous police agencies fared in this surprise scenario.

We also explore the subject of youth engagement and how RCMP outreach initiatives are drawing young Canadians and vulnerable communities into the national security conversation.

The RCMP's National Security Criminal Investigations (NSCI) outlines the recent positive changes that have occurred there, including the successful disruption of significant terrorist targets in 2006–2007. Read about the current and future improvements at NSCI.

We hear from two other areas of the RCMP — the Immigration and Passport Special Investigation Section and the Canadian Air Carrier Protective Program — to find out how these specialized teams help protect Canada's national security both inside and outside its borders.

In this issue, we hear from our law enforcement partners who continue to be engaged in supporting the national security priority.

Alain Goudreau of the Centre for Security Science at Defence Research and Development Canada describes the complex but essential task of establishing an all-hazards risk assessment picture for the Government of Canada. Learn about the study that will help assess Canada's ability to respond to a wide range of security threats.

Also, Brent Smith of the Terrorism Research Center at the Fulbright College, University of Arkansas, analyzes terrorist behaviour in the U.S. based on past attacks. He proposes that understanding their patterns might help police prepare for future attacks.

The Internet has become a powerful tool for terrorists, victims and law enforcement agencies alike.

Professor Gabriel Weimann of the University of Israel draws upon his extensive research into terrorists' use of the Internet to describe the latest trend — narrowcasting — for targeting a specific audience.

Canadian journalist Peter Zimonjic was living in London and travelling on the city's subway the day of the July 7 bombings. Deeply affected by what he experienced, he launched a victim support website and, this year, released a book chronicling the bombings through the eyes of survivors. His Q&A with the *Gazette* touches on the role the website played in allowing victims, including police, to find support.

Meanwhile, Michael Wertheimer of the U.S. Office of the Director of National Intelligence writes about how the challenges facing the intelligence community are pushing its members to explore new ways to perform analysis — using Web 2.0.

Finally, in our regular departments, learn from an expert in tactical communication, read about a pilot project on the use of head cameras by U.K. police, and find out more about police fatigue and how it can be better managed.

You can view all these articles online, and many past issues, at ***www.rcmp-grc.gc.ca/gazette/index.html.***

Katherine Aldred

More to explore on national security from the Canadian Police College Library
www.cpc.gc.ca/library_e.htm

Books

Canadian Police College. *Emerging International Threats: A Police Perspective / Nouvelles menaces internationales: la perspective policière*. Ottawa, Canada: 2007. VL 2009. HV 7431 Em3.

Hamilton, Dwight. *Inside Canadian Intelligence: Exposing the New Realities of Espionage and International Terrorism*. Toronto, Canada: Dundurn Press, 2006. JL 86 I58 H18.

Munn-Venn, Trefor. *A Resilient Canada: Governance for National Security and Public Safety*. Ottawa, Canada: Conference Board of Canada, 2007. HV 6419 R31.

Riordan Raaflaub, Tim. *Civilian Oversight of the RCMP's National Security Functions / Surveillance civile des fonctions de la GRC en matière de sécurité nationale*. Ottawa, Canada: Parliamentary Information and Research Service, 2006. HV 7641 R11.

Standing Committee on National Security and Defence. *Borderline Insecure*. Ottawa, Canada: 2005. HV 7955 C16.

Articles

Herzog, Jeffrey Owen. "Using Economic Intelligence to Achieve Regional Security Objectives." *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 2, (Summer 2008): p. 302–313.

Razavy, Maryam. "Sikh Militant Movements in Canada." *Terrorism and Political Violence*, Vol. 18, No. 1, (Spring 2006): p. 79–93.

On guard for national security

A terrorist bomb. Web-based terror tactics. A high-level security breach. A major financial fraud. These are but a few of the scenarios that can have a direct and serious impact on national security.

In this issue, we look at how law enforcement agencies are arming themselves with the knowledge and skills to prevent and prepare for such incidents, and respond effectively when they do occur.

In our cover article, writer Caroline Ross looks at the increasing threat from domestic extremists in Canada — and the RCMP's role in investigating cases with possible terrorist links. Read about what it takes to build top-quality investigations when it comes to suspicious terrorist activities.

Preparing for a national security incident is a complex task in today's borderless world. The *Gazette* was on hand to observe a day-long emergency response exercise involving three simultaneous attacks in Hamilton, Ontario. Find out how the more than 100 first responders from numerous police agencies fared in this surprise scenario.

We also explore the subject of youth engagement and how RCMP outreach initiatives are drawing young Canadians and vulnerable communities into the national security conversation.

The RCMP's National Security Criminal Investigations (NSCI) outlines the recent positive changes that have occurred there, including the successful disruption of significant terrorist targets in 2006–2007. Read about the current and future improvements at NSCI.

We hear from two other areas of the RCMP — the Immigration and Passport Special Investigation Section and the Canadian Air Carrier Protective Program — to find out how these specialized teams help protect Canada's national security both inside and outside its borders.

In this issue, we hear from our law enforcement partners who continue to be engaged in supporting the national security priority.

Alain Goudreau of the Centre for Security Science at Defence Research and Development Canada describes the complex but essential task of establishing an all-hazards risk assessment picture for the Government of Canada. Learn about the study that will help assess Canada's ability to respond to a wide range of security threats.

Also, Brent Smith of the Terrorism Research Center at the Fulbright College, University of Arkansas, analyzes terrorist behaviour in the U.S. based on past attacks. He proposes that understanding their patterns might help police prepare for future attacks.

The Internet has become a powerful tool for terrorists, victims and law enforcement agencies alike.

Professor Gabriel Weimann of the University of Israel draws upon his extensive research into terrorists' use of the Internet to describe the latest trend — narrowcasting — for targeting a specific audience.

Canadian journalist Peter Zimonjic was living in London and travelling on the city's subway the day of the July 7 bombings. Deeply affected by what he experienced, he launched a victim support website and, this year, released a book chronicling the bombings through the eyes of survivors. His Q&A with the *Gazette* touches on the role the website played in allowing victims, including police, to find support.

Meanwhile, Michael Wertheimer of the U.S. Office of the Director of National Intelligence writes about how the challenges facing the intelligence community are pushing its members to explore new ways to perform analysis — using Web 2.0.

Finally, in our regular departments, learn from an expert in tactical communication, read about a pilot project on the use of head cameras by U.K. police, and find out more about police fatigue and how it can be better managed.

You can view all these articles online, and many past issues, at ***www.rcmp-grc.gc.ca/gazette/index.html.***

Katherine Aldred

More to explore on national security from the Canadian Police College Library
www.cpc.gc.ca/library_e.htm

Books

Canadian Police College. *Emerging International Threats: A Police Perspective / Nouvelles menaces internationales: la perspective policière*. Ottawa, Canada: 2007. VL 2009. HV 7431 Em3.

Hamilton, Dwight. *Inside Canadian Intelligence: Exposing the New Realities of Espionage and International Terrorism*. Toronto, Canada: Dundurn Press, 2006. JL 86 .I58 H18.

Münn-Venn, Trefor. *A Resilient Canada: Governance for National Security and Public Safety*. Ottawa, Canada: Conference Board of Canada, 2007. HV 6419 R31.

Riordan Raatlaub, Tim. *Civilian Oversight of the RCMP's National Security Functions / Surveillance civile des fonctions de la GRC en matière de securité nationale*. Ottawa, Canada: Parliamentary Information and Research Service, 2006. HV 7641 R11.

Standing Committee on National Security and Defence. *Borderline Insecure*. Ottawa, Canada: 2005. HV 7955 C16.

Articles

Herzog, Jeffrey Owen. "Using Economic Intelligence to Achieve Regional Security Objectives." *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 2, (Summer 2008): p. 302–313.

Razavy, Maryam. "Sikh Militant Movements in Canada." *Terrorism and Political Violence*, Vol. 18, No. 1, (Spring 2006): p. 79–93.

GAZETTE

Vol. 70, No. 3, 2008

A Royal Canadian Mounted Police Publication

Strong inter-agency relationships are key when national security is at stake

Cover

National security

8 Protecting Canadians from domestic terrorism
11 Exercising a joint counterterrorism plan
14 The future of National Security Criminal Investigations
16 Reducing security threats from employees abroad
17 Youth outreach on national security
18 Survivor looks back on London transit bombings
19 The Canadian Air Carrier Protective Program
20 Conducting an all-hazards risk assessment
22 Online terrorists target children and women
24 A look at terrorist behaviour
26 Arming intelligence with Web 2.0

Departments

2 Editorial message
4 News notes
6 Q&A with Dr. George Thompson, an expert in tactical communication
12 Panel discussion — Is national security today overly focused on terrorism?
28 Just the facts
29 Featured submission — Canadian experts help with Guatemalan investigation
30 Featured submission — Managing police fatigue
32 Featured submission — The pros and cons of body-worn video
34 On the leading edge
36 From our partners — Threat assessment unit in Alberta targets domestic violence
38 Emerging trends — Vancouver Police and virtual recruiting

ON THE COVER

Members of the Hamilton Police Service Emergency Response Unit assess the situation on a hijacked train during a counterterrorism exercise in Hamilton, Ontario, in May 2008. The exercise involved over 110 participants from three municipal police forces, the RCMP and several federal, provincial and municipal partners, proving that protecting national security really is a collective effort.

Photo: Caroline Ross

PUBLISHER – Nancy Sample EDITOR – Katherine Aldred WRITER – Caroline Ross GRAPHIC DESIGN – Jennifer Wale
ADMINISTRATIVE SUPPORT AND CIRCULATION – Alexandre Guilbeault TRANSLATION – RCMP Translation Services PRINTING – Performance Printing

GAZETTE EDITORIAL BOARD

S/Sgt Lori Lynn Colbourne - Insp Craig Duffin - Dr. Edward Drodge - Sgt Chris Fraser - Wendy Nicol - Dr. Roberta Sinclair - Dr. Brian Yamashita

The *Gazette* (ISSN 1196-6513) is published in English and French by the Public Affairs and Communication Services of the Royal Canadian Mounted Police in Ottawa. Cover design and contents are copyrighted and no part of this publication may be reproduced without written consent. Canada Post Publications Mail Agreement 40064068. The *Gazette* is published four (4) times a year and is issued free of charge on a limited basis to accredited police forces and agencies within the criminal justice system. Personal subscriptions are not available. The *Gazette* welcomes contributions, letters, articles and comments in either official language. We reserve the right to edit for length, content and clarity. HOW TO REACH US : Editor — RCMP Gazette, L.H. Nicholson Building, Rm A200, 1200 Vanier Parkway, Ottawa, Ontario, CANADA K1A 0R2. Phone: (613) 998-6307, E-mail: gazette@rcmp-grc.gc.ca, Fax: (613) 993-3098, Internet: ***www.rcmp.ca/gazette/index.html***,

© Ministry of Public Works and Government Services (2000).

MAKING A DIFFERENCE IN AFGHANISTAN

Canadian police have been serving in Afghanistan since 2005, but are they making a difference? You bet they are, if the experiences of two recently returned RCMP officers are any indication.

Supt Paul Young and Cpl Barry Pitcher returned to Canada in February 2008 after spending a year in Afghanistan training and mentoring local police forces.

Young spent his year in Kabul, providing strategic and operational advice to the Chief of the Kabul Police. He helped reorganize the 10,000-officer force — which initially had no divisions or command hierarchy — into four smaller units headed by subordinate commanders.

"We reduced (the police chief's) span of command from thousands down to about 30 or 40 people," says Young. "Manageable."

Young also spearheaded projects to rebuild Kabul's 30 ramshackle police stations. One project — building a rock wall around the police headquarters — was completed mere weeks before a bus explosion outside the station killed 35 officers.

"Had the rock wall not been there, we probably would have lost two or three hundred more," says Young.

Closer to the front lines, Pitcher served in Kandahar with the Canadian Provincial Reconstruction Team. He and five other Canadian police officers developed and ran training courses for the Afghan National Police (ANP), covering topics like first aid, IED detection and crime scenes.

Many of Pitcher's students didn't know how to apply pressure to a bleeding wound, let alone how to identify a mine. When they graduated, some were so happy they hugged him.

"Over there, it was the little things," says Pitcher. "Those are the things that will really reciprocate long after you're gone."

Canadian police are also planting the seeds of community-based policing in Kandahar, says Pitcher. It's a gradual process, given the ANP tendency to patrol with a heavy hand, weapons drawn.

"We try to tell them, 'Sling your rifle, bring a box of wool hats (and) give them out to some of the children, distribute flyers that tell children how to stay away from mines and IEDs, give the village elder a cell phone. You're building relationships."

Canadian Forces Combat Camera

RCMP Cpl Barry Pitcher (left) congratulates members of the Afghan National Police upon their graduation from a vehicle checkpoint training course in April 2007.

To learn more about Canadian police efforts in Afghanistan, visit ***www.rcmp.ca/peace_operations/afghanistan_e.htm.***

—Caroline Ross

EXCHANGE BRINGS CULTURAL AWARENESS

The Nunavut RCMP and the Ottawa Police Service (OPS) have launched an officer exchange program to improve cultural and career connections for officers working in Inuit communities.

In March 2008, two OPS officers travelled to Nunavut — homeland of Canada's Inuit population — for month-long postings at RCMP detachments in remote Inuit communities. The Nunavut RCMP will send two Inuit-based officers to Ottawa on a reciprocal exchange later this year.

Sgt Mike Toohey of the Nunavut RCMP says the two police forces were a natural fit because Ottawa has one of the largest Inuit populations outside Nunavut.

"We would be able to send our Inuit members down to a municipal police force to get trained and exposed to that type of reality, and at the same time, we'd be able to provide cultural training for members of the Ottawa Police Service, so they would be more aware of that segment of the population," says Toohey.

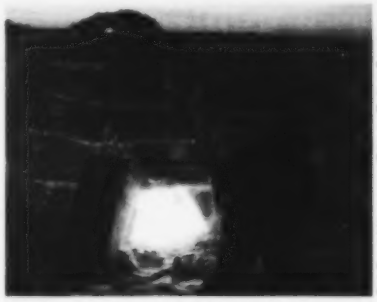
During their exchange, the OPS officers were posted in Clyde River and Hall Beach, populations 820 and 654. When not on duty, the officers learned about Inuit culture from local guides.

OPS Sgt Brad Hampson was stationed in Clyde River. He says the exchange helped him appreciate the "culture shock" that Inuit people experience when they arrive in Ottawa.

"They come here wide-eyed and awestruck. Never seen trees. Never seen (shopping centres)," he says. "They're very susceptible to temptations (like alcohol, drugs and gangs)."

Since his exchange, Hampson has made connections with Inuit residential facilities in Ottawa and helped organize a police-Inuit open house to improve the lines of communication between Ottawa police and the local Inuit community.

RCMP Cst Chris Boyd works in the Clyde River detachment and says Hampson's visit gave him insight into urban policing and the opportunities it presents.



Sgt Brad Hampson, Ottawa Police Service

Ottawa Police Service Sgt Brad Hampson and his Inuit guide (pictured) built and slept in this igloo as part of Hampson's month-long exchange at the RCMP detachment in Clyde River, Nunavut.

Boyd says many Nunavut RCMP officers — himself included — are junior members whose policing experience is limited to isolated northern detachments. He says an exchange to Ottawa would help officers like him prepare for postings in urban centres, where street names and traffic signs are normal, police use equipment like Breathalyzers and video surveillance, and officers don't know everyone in town.

—Caroline Ross

WOULD YOU LIKE FRIES WITH THAT?

Drunk drivers who grab a late-night snack on the way home from the bars in Surrey, British Columbia, might get more than a side of fries with their fast food orders. They might be arrested for impaired driving, courtesy of an RCMP officer in the drive-thru window.

In a novel approach to drinking and driving counterattack, the Surrey RCMP Traffic Section has partnered with local fast food restaurants to position undercover officers in late-night drive-thrus on weekends, when the bar crowds head home. The plainclothes officers sit in the drive-thru windows with restaurant staff, watching drivers for signs of impairment like slurred speech or the odour of alcohol. If an officer sees something suspicious, he or she radios a uniformed partner who waits off-site in a marked patrol car, ready to intercept suspect drivers once they leave the restaurant property.

"It's all about the element of surprise," says Cst Brian Nanton of the Surrey Traffic Section Problem Solving Team.

Nanton remembers his first shift in a drive-thru, when he watched a driver pull up to the window and take a swig from an open alcoholic beverage. "It's amazing how many people are carefree about (drinking and driving)," he says. "You don't really see how many people actually do that until you get behind the scenes."

The initiative — dubbed Project WULF for "Would you Like Fries" — has been running since summer 2007, with the RCMP tailoring operations according to season and resources.

As of spring 2008, WULF had resulted in approximately two dozen 24-hour licence suspensions and three arrests. But the numbers don't tell the full story, says Nanton.

"The main goal was to put the word out there," he says, adding that once the media picked up the story, the initiative grew its own legs. "(People) think the police are at every drive-thru on the weekend. It's putting the fear into people that they shouldn't be driving drunk."

Courtesy of Surrey Now

He won't hand you fries, but he could hand you an impaired driving charge. Cst Brian Nanton and the Surrey RCMP Traffic Section look for impaired drivers at late-night drive-thrus.

—Caroline Ross

ALBERTA RCMP GOING GREEN

If you were to rate Alberta municipalities and the RCMP on their "green" policing infrastructure, they'd get two silvers and a gold.

The rankings come courtesy of three recently constructed RCMP detachments in Grande Prairie, Hinton and the Regional Municipality of Wood Buffalo. Each detachment was designed and built under the Leadership in Energy and Environmental Design (LEED) initiative managed by the Canada Green Building Council. To obtain LEED rankings — bronze, silver, gold or platinum — new or renovated buildings must meet specific environmental criteria in areas like sustainability, water efficiency, energy and atmosphere, and materials and resources.

In Wood Buffalo, the new LEED-gold building is set to open in September 2008. It features a solar wall to capture heat, a "glass spine" to enhance natural light, individually ventilated workstations, and adjustable workstation walls to facilitate future growth.

"The flexibility for the RCMP and their needs in this community were paramount in the design (of the building)," says Cherie Cormier, Wood Buffalo municipal project lead.

Cst Janice Acourt of Wood Buffalo RCMP marketing and promotions hopes that the trend-setting building will help attract experienced officers to the growing northern municipality.

The Hinton detachment, which opened in March 2007, uses the region's naturally cold water for domestic cooling. It also meets RCMP operational requirements, thanks to significant input from RCMP members during the design of interview rooms, exhibit facilities, access points and other key areas.

"The input (we had) into the building was fantastic," says Hinton RCMP Sgt Brenda Burns. "Our objective is to get a functioning police building, and the green part is an absolute bonus."

In Grande Prairie, where recovered heat warms an underground tunnel to the courthouse, RCMP officers have already made use of the detachment's adjustable workspace configurations to accommodate new members. The green detachment opened in July 2006.

There are several other LEED-registered RCMP projects underway across Canada, including a new headquarters building for over 2,500 RCMP employees in Surrey, British Columbia. For more information on the LEED initiative, visit ***www.cagbc.org***.

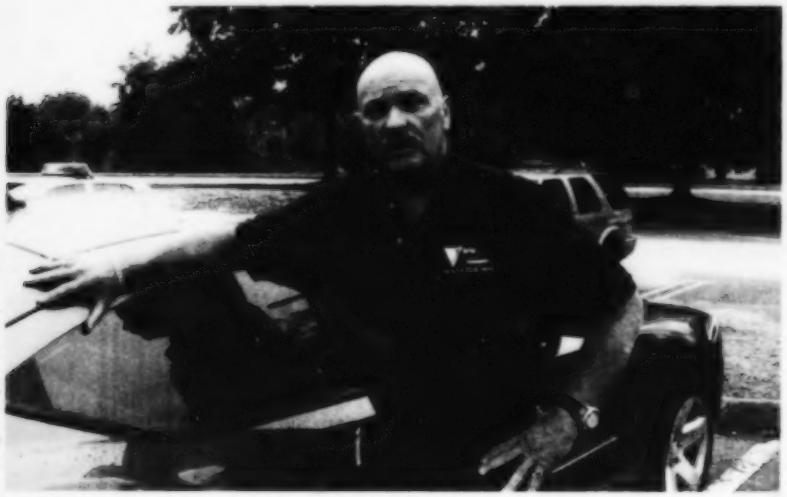
—Caroline Ross

This new RCMP detachment in the Regional Municipality of Wood Buffalo, Alberta, will include a solar wall to capture heat and a "glass spine" to enhance natural light.

Cst Terry Hanna

The art of Verbal Judo

Using words to generate voluntary compliance



J.J. King, Raleigh Police Department

George Thompson says Verbal Judo teaches officers to stay calm under verbal assault, deflect the assault, listen, and use words to obtain co-operation.

As a beat officer, your most powerful weapon isn't your gun or your baton, it's the words that come out of your mouth, says Dr. George J. Thompson, PhD, former police officer and founder of the Verbal Judo Institute, a tactical communication training centre based in Auburn, New York. Thompson's books and training courses have taught over 700,000 police officers how to use words to their advantage. He recently shared some tips and techniques with Gazette *writer Caroline Ross.*

What is tactical communication?

It's also called Verbal Judo, "verbal" being words and strategies of persuasion and "judo" being the art of redirecting behaviour. It's really a martial art of the mind and the mouth, where we teach people to stay calm under verbal assault, to deflect verbal assault and to see in the assault itself the seeds of a resolution.

How does tactical communication impact police work?

Prior to Verbal Judo, a person dealing with the police had three options: fight, flight or surrender and lose face. Verbal Judo presents a fourth option: choose to go with dignity, because it's good for you. And before Verbal Judo, if you (as a police officer) were insulted, there were only two things you could do: get sucked in by the other person's dynamics or ignore it until you snap. We teach a third: deflect, listen tactically and move forward with pride and dignity.

What mistakes do police officers make with regards to tactical communication?

Cops almost always react to what is said to them rather than what is meant, and they almost always react to tone and attitude. A cop who walks up to a car and is told, "Hey, you doughnut-eating son-of-a-gun!" — if he reacts to that insult, the citizen now controls him because he (the citizen) controls the tenor of the discussion. We teach cops to let attitude drift, because you can't change attitude at the time anyway. You have to deflect the words and focus on the meaning.

How do you deflect a verbal assault?

We use certain phrases to deflect attacks. I usually say use two or more because it sounds natural. They're things like, "Sir, I can see you're upset, but . . . ," "I'm sorry you feel that way, but . . . ," "I appreciate what you're saying and I understand it, but . . . ." Rather than react to the words, you quickly respond with phrases that get you to the word "but," which then becomes a focus word. Everything you say after that word "but" must be professional language tailored and aimed at the goal of generating compliance or co-operation.

How do you determine the real meaning behind the words?

We teach tactical listening skills. Listen to what people are giving you to work with rather than what they're saying. Like the angry driver who's complaining about being late for a meeting and calling you all kinds of names. What you know is that he's late and time is of the essence. So I would say, "Sir, I can see you're upset and I'm sorry; however, we can do this quickly and efficiently and get you to that meeting as quickly as possible." Another guy says, "I can't go to jail! I don't want my family to find out about this!" So he's a family man; I've got something to work with now. People will unwittingly fill your pockets with intelligence as to how to handle them, if you only listen.

How do you then use words to obtain compliance and co-operation?

I teach a five-step method of persuasion. Step one: ask for co-operation: "Sir, could I ask you to step over here for me please?" Two, if you get resistance, always tell them why — set the context: "Let me tell you why I'm asking you to move from the car, sir." Three, create and present options. Put the positive options first, followed by the negative, and end with a positive clip. Your voice has to be pleasant, and you have to be very specific: "Sir, you were going somewhere today, weren't you? I'd like to see you get home. I want you to be able to be home with the family, be with the family, sleep with the family, get up in the morning

and continue your day. That's what I want for you. Let me tell you something, sir. If you don't step out of the car so I can search it for contraband, we have to place you under arrest. Then you'll go to jail, you'll spend your time with us tonight and you'll be out sometime tomorrow afternoon. And that's $300 for the tow. I don't think you need that, sir, so work with me. You don't need that kind of trouble, that kind of expense." See how I ended positive? The fourth step, (if there is still resistance), is really quite unique. The fourth step is to confirm: "Sir, is there anything I could say to get you to step from the vehicle? I'd like to think so." That last phrase is crucial. No threat, perfectly pleasant, but notice I've said, "Will words work?" He can save face and still comply. If he says no, the fifth step is act: arrest, control, transport. Words are over now.

What about body language?

Research shows that only seven to 10 per cent of your total impact on somebody is content. Thirty-three to 40 per cent is your verbal personality, which is your voice as heard by the other. And 50 to 60-plus is other non-verbals, which means body language, facial expressions and proxemics. If you say the right thing the wrong way, you're done.

Any other tips?

The average policeman could change the entire response he gets by simply starting every verbal encounter he can with "How can I help you?" And part of that is (saying) "could I ask" rather than telling people what to do. "Sir, could I ask you to step over here for me please?" (rather than "Hey, come over here!") Everybody likes to be asked; nobody likes to be told. And if you listen tactically, you have the advantage. You no longer get upset when you get attacked. You smile inwardly and say, "Now I gotta listen, because he will tell me how to handle him." Already, we move from verbal attack as a crisis to verbal attack as an opportunity. ■

For more information on Verbal Judo, visit ***www.verbaljudo.com***.

THE MEET AND GREET

"Driver's licence, please!" Beginning a verbal encounter with an order like this is sure to generate resistance, says Dr. George Thompson, founder of the Verbal Judo Institute. Instead, try Thompson's eight-step meet-and-greet, illustrated below with the example of a routine vehicle stop.

1. **Give a greeting**: "Good morning/afternoon/evening."
2. **Identify yourself and your department**: "Officer Thompson, Syracuse PD." Providing your name shows fearlessness,confidence and professionalism, and also makes it harder for the person to insult you. Providing the department name adds power.
3. **Give the reason for the stop**: "Sir, the reason I stopped you today is I did notice that you failed to stop at the stop sign at Third and Market."
4. **Ask for justification**: "Is there some justified reason for failing to stop at that sign today, sir?" Pause for the first time. By providing your name and reasons up front, you reduce the grounds for resistance. Watch and listen to the person's response for clues on how to handle him.
5. **Ask for a driver's licence (or other identification)**. If you suspect the person is armed, ask: "Sir, do you have your registration and insurance with you; if so, where do you keep it in the vehicle?" followed by, "Is there anything in that area that might cause me concern?" Watch the person's reaction for hesitation or other signs that he's hiding something.
6. **Ask for any necessary clarification**. Then ask the person to remain in the vehicle while you "evaluate" your information. The word "evaluate" is less threatening than phrases like "check you out."
7. **Provide your decision** (warning, ticket, notice of next steps, etc.).
8. **Close on a positive note**. "Thank you for your co-operation, sir. Do drive carefully."

The threat from within

Protecting Canadians from domestic terrorism

Guylain Ouellette

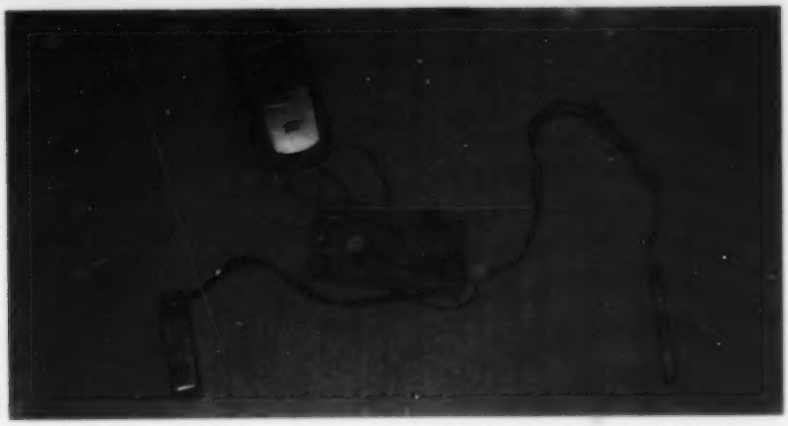
By Caroline Ross

On June 2, 2006, Canadian police arrested 17 Toronto residents for allegedly plotting to bomb Toronto infrastructure, behead Canadian politicians and commit other acts of al-Qaida-inspired extremism.

It wasn't the first time that Canada has been targeted by domestic extremists — the FLQ, Squamish Five and Air India incidents spring to mind* — but the Toronto arrests do suggest a new threat from within, and one that will continue to grow as Canada becomes more active in global hot spots like Afghanistan and Darfur, and as the Internet brings extremist ideology into everyone's living room.

"Domestic terrorism is probably a bigger threat to Canada now than it has ever been," says A/Commr Bob Paulson, head of RCMP National Security Criminal Investigations (NSCI) in Ottawa. "We have Canadians right now, as we speak, in Northwest Pakistan, at training camps, who have stated their intention to attack us here in North America. That's what we have to worry about."

In Canada, the RCMP holds jurisdiction in matters involving national security. NSCI is currently investigating over 800 cases with possible terrorist links. Since 9/11, they've been successful in staying one step ahead of the extremists, and



Caroline Ross

Modern-day terrorists construct explosive devices from everyday materials such as those pictured. National security investigators seized similar items during their investigation of the 17 Toronto residents arrested on June 2, 2006.

they've implemented a string of measures to help keep it that way.

"Cadillac" investigations

"One of my priorities is to ensure that we have absolute 'Cadillac' (top-quality) investigations when it comes to suspicious terrorist activities," says Paulson. "We cannot afford to fail even once in terms of getting in front of the terrorist threat."

Staying in front of that threat requires significant resources — more so than for other types of criminal investigations — because investigators must keep constant tabs on several key targets and treat every suspicious incident as if it were real.

"Basically, we're doing a threat assessment every day: What are these targets doing? Do we have the level of coverage that we need? Do we have the appropriate resources in the appropriate places?" says Supt Jamie Jagoe, who oversees national security investigations in Ontario. "We have to have a level of comfort that we can respond at any given moment to the threat."

That level of comfort comes courtesy of partner agencies like the Canadian Security Intelligence Service, the Canada Border Services Agency, Citizen and Immigration Canada and municipal police forces. Specialists from these agencies co-exist with the RCMP in four Integrated National Security Enforcement Teams (INSETs). Based in Toronto, Montreal, Ottawa and Vancouver, the INSETs handle all national security investigations in Canada.

The Toronto INSET currently employs 125 officers, including 50 seconded from 11 partner agencies. In the seven months leading up to the June 2 arrests, that total swelled to 700, including 84 full-time investigators at the peak of investigation and 400 officers on the day of the arrests.

It's strength in numbers, and it keeps those "Cadillac" investigations on the road.

One voice across the globe

Almost every domestic terrorism investigation has international connections, says Supt Rick Reynolds, recently retired director of the RCMP National Security Criminal Operations Branch.

Canadian extremists may receive funding, equipment, information, training or ideological direction from individuals in other countries. Unfortunately, says Reynolds, many of those countries are third world or failed states with questionable human rights records.

"All you have to do is go to the O'Connor inquiry. . . and you'll see the risks and responsibilities associated with sharing information with foreign agencies," says Reynolds, referring to a 2004 government inquiry into the role Canadian officials played in the case of Maher Arar. Arar, a Canadian citizen, was detained in the United States and deported to Syria, where he was interrogated and tortured as a suspected terrorist. According to the O'Connor inquiry's final report, "it is very likely that, in making the decisions to detain and remove Mr. Arar, American authorities relied on information about Mr. Arar provided by the RCMP, . . . some of which portrayed him in an inaccurate and unfair way."

In the wake of the O'Connor inquiry, NSCI implemented a central governance framework to oversee all national security investigations. Responsibility for foreign relations rests with the headquarters component, where a dedicated team ensures that information exchanged with other countries is accurate, relevant, legally sound and bound by appropriate caveats.

"It brings a high degree of accountability and consistency," says Reynolds, and that helps NSCI co-operate with foreign agencies on matters of mutual security while still protecting the values of Canadian society.

A court precedent?

INSET investigators constantly struggle with the fact that Canadian police forces and Canada's security intelligence agency are bound by different disclosure requirements.

Police agencies, as part of the Crown, are required to fully disclose all information relevant to criminal proceedings. The Canadian Security Intelligence Service (CSIS), a civilian organization, is not bound by the same requirement. However, CSIS regularly provides the RCMP with information that could factor into national security investigations.

For INSET investigators, it can be a long, complicated, sometimes impossible process to bring information provided by CSIS forward as court-approved evidence — even during preliminary applications for search warrants or wire taps. But as the first adult in the Toronto case goes to trial, that situation could change.

"The defense are bringing a motion to have CSIS required to disclose through the Crown prosecutor on the same basis as the RCMP are required to disclose," says

Debra Robinson, senior counsel with RCMP legal services.

The motion is scheduled to be heard in December 2008, and it could revolutionize Canadian court disclosure processes.

"This is very novel," says Robinson. "It's going to be interesting to see what the court does."

Eyes, eyes everywhere

National security investigators can't be everywhere all the time, hunting for signs of potential terrorist attacks. It helps to have people at ground-level aware of what to look for and what to do if they see something suspicious.

In April 2008, the RCMP launched a Suspicious Incident Reporting system for critical infrastructure targets like subways and oil pipelines. Currently operating on a pilot basis, the system allows pre-authorized infrastructure stakeholders across Canada to file incident reports in a secure central database. RCMP intelligence analysts regularly review the reports for linkages and escalate items accordingly.

NSCI is also working to create a national network of Counter-Terrorism Information Officers (CTIOs) — officers who are attuned to national security threats, indicators and processes and can educate front-line staff and funnel relevant observations to the INSETs. The goal is to get front-line officers thinking "national security" on a regular basis, says Sgt Steve Corcoran, who created the program and has trained over 100 CTIOs in British Columbia.

Corcoran's network spans RCMP districts, municipal police services and external agencies like B.C. Corrections, the B.C. Conservation Officer Service and the Department of Fisheries and Oceans. You need only look at the Toronto case to see the value of external partnerships, says Corcoran.

"(The Toronto suspects) went out into the bush to set up a camp. . . . Fisheries officers and conservation officers are as likely to find that as (police) are, so they have to know what to look for."

Looking upstream

Perhaps the best way to tackle the threat of domestic terrorism is for police to build strong community partnerships and involve community members in solutions to domestic radicalization.

That's certainly what RCMP Insp Jim Stewart and his team are hoping. Stewart chairs a multi-agency working group involving stakeholders from the Government of Canada, the Canadian Association of Chiefs of Police and police forces from Victoria to Halifax. Together, the partners are developing a pan-Canadian counter-radicalization strategy, based on similar initiatives in the United Kingdom.

"(This will be) a very Canadian program, one that has been fine-tuned to provide the best benefit to communities across Canada when it comes to recognizing and countering radicalization that leads to violence," says Stewart.

The strategy will incorporate several existing NSCI outreach initiatives, such as local community advisory groups that helped quell community concerns in the wake of the June 2 arrests. Stewart also hopes to deliver elements of the strategy through the CTIO network.

"What's key right now is that the time is right," says Stewart. In the post 9/11 environment, Canada has not experienced a terrorist attack, so the RCMP and its partners aren't building relationships in crisis mode. "If we can start to look upstream before (terrorist acts occur), we're preventing. It's all about making sure that there's a non-event." ■

** In October 1970, members of the Front de libération du Québec (FLQ) kidnapped two government officials, murdering one. In 1982, five Canadians bombed infrastructure targets in British Columbia and Ontario before being apprehended near Squamish, British Columbia. In June 1985, an Air India flight originating in Montreal exploded in mid-air, killing all 329 passengers. Canadian residents later stood trial for planting a suitcase bomb.*

Gyjan Ouellette

This Toronto subway station is one of many Canadian critical infrastructure sites that will benefit from a new Suspicious Incident Reporting system, which allows infrastructure stakeholders, the RCMP and other government, intelligence and law enforcement partners to share information on potential security threats of a criminal nature.

110 responders vs. eight extremists

Testing the response

By Caroline Ross

Here's the scenario: Armed extremists hijack a train and a boat in a busy Canadian port city. The train sets off for Toronto with a chemical weapon on board. The boat, stocked with explosives, heads for a major bridge during rush hour. Other extremists hole up in a warehouse at the pier, guns, hostages and bombs at the ready.

Could it happen? It did on May 27, 2008, in Hamilton, Ontario.

It was all part of Operation Midnight Express, a day-long emergency response exercise co-ordinated by the Hamilton Police Service (HPS) and involving over 110 first responders from the Hamilton, Halton and Niagara municipal police services; the RCMP; Canadian Pacific Rail; the City of Hamilton; Hamilton fire and emergency services; and the Hamilton hospital.

"We wanted to test interoperability, to further develop partnerships," says HPS Supt Paul Morrison, who chaired the exercise planning committee. "And we needed to address growing threats within our community."

Morrison and his team designed the exercise to occur in real-time, with participants having little or no prior knowledge of the situation. Events escalated from a seemingly routine single-vehicle collision to a full-blown extremist incident spanning multiple sites, with a joint incident command team headed by HPS Deputy Chief Ken Leendertse.

While Morrison acknowledges that responsibility for extremist incidents usually falls to the RCMP under its national security portfolio, he says it's important to test the local response in the event that the federal police can't immediately attend the scene.

Supt Jamie Jagoe, head of RCMP national security investigations in Ontario, agrees. "It's important to stretch the police response, because in the real world, things can get very complex. The goal here is to ensure the systems and synergies are in place."

As the day progressed, those systems and synergies were put to the test. Tactical teams from Hamilton, Halton and Niagara synched up with the RCMP Marine Security Emergency Response Team to conduct simultaneous assaults on the train, warehouse and vessel. Municipal forces practised using a radio interoperability system provided by the RCMP — ironing out some kinks along the way. Transport Canada provided crucial information on how to safely divert marine traffic during the marine assault. And Hamilton medical services performed a casualty triage, testing the lines of communication between first responders and hospital staff.

There were some challenges along the way — the warehouse assault was delayed by a communications snag, for example — but the exercise proved that federal, provincial and local responders can pull together and successfully problem-solve in crisis mode, says Morrison. He credits a cohesive, well-informed joint command-and-control structure for much of the success in that regard.

Caroline Ross

Deputy Chief Ken Leendertse of the Hamilton Police Service co-ordinated the efforts of over 110 first responders during a counter-terrorism exercise in Hamilton, Ontario, last May.

With the exercise and debrief now complete, HPS hopes to share its experience through a one-day training forum for commanders at the Ontario Police College.

"There is a high need to give this sort of information to other police agencies so that they can, in future, plan better," says Morrison. He adds that live video footage of the exercise, captured by the Ontario Police Video Training Alliance, will help highlight lessons learned.

Morrison invites police forces interested in conducting similar exercises to contact him at the Hamilton Police Service. ■

Planning a national security exercise in your jurisdiction?

Members of the Operation Midnight Express (OME) planning committee offer these tips:

- Keep the scope within your agency's responsibilities and capabilities.
- Learn from agencies that have held similar exercises.
- Seek alternate funding from sources like the Government of Canada Joint Emergency Preparedness Program.
- Start planning early, and expect a lengthy planning process. Planning for OME lasted eight months.
- Use a standard operational planning format, and include an evaluation plan.
- Staff your planning committee according to expertise, not rank.
- During the exercise, run a "simulation cell" to monitor and control scenarios. Stagger attendance to ensure staff remain alert at critical moments.
- Don't be bound by expected outcomes.

Is national security overly focused on terrorism?

The panellists

A/Commr Bob Paulson, National Security Criminal Investigations, RCMP
Senator Colin Kenny, Standing Senate Committee on National Security and Defence, Canada
Norman Inkster, Chair of the Advisory Council on National Security for the Prime Minister of Canada

A/Commr Bob Paulson

Excellent question for our time. I say no. I ask whether the way we currently focus on national security is impeding our ability to conduct effective counterterrorism operations. I struggle with that answer because I think it is yes.

Let's review what it was that led us to our current interest in national security. Terrorists hijacked airplanes and drove them into buildings in the United States. Elsewhere in the world, terrorists blew up trains, subways and nightclubs. Terrorists continue to plan and conspire to commit attacks. Canada has been named as a target by al-Qaida but has not yet been attacked. The threat remains. Remarkably, it has evolved to where some of our own citizens, radicalized to criminal conduct, are now the subject of our interest. Canadians travel to Pakistan to train in terror.

National security is at the heart of any government's mandate and we all have a primary duty to protect our citizens. Societies have an obligation to provide security from threats against the state. National security is not easily defined. Economic security, border integrity, space activity, energy, infrastructure, agriculture, health and more all factor in to the security of a nation. To me, the nature and imminence of the threat ought to orient our focus in deciding how to secure ourselves. Terrorism is much more than a spot on the "probability-versus-impact" spectrum. Terrorists want more than just to hurt us; they want to fundamentally change who we are.

At a time when the threat to national security is manifest, as it is now because of terrorism, I suggest we should focus on dealing with the immediacy of this threat before focusing any further on the broader range of issues affecting our security (beyond our current attention to these areas). It's not the time to be browsing the catalogue for sprinkler systems when the arsonist is about to set the fire.

All terrorist acts are criminal and so criminal justice must figure prominently in our response. The terror investigation is a must-win proposition and requires perfection in today's highly challenging and complex criminal justice landscape. Public confidence in our institutions hangs in the balance. Therefore, an effective counterterrorism response for Canadians must include the following:

- A fully integrated and comprehensive national community outreach and counter-radicalization program
- An effective intelligence capacity, aligned with the criminal justice reality, and providing timely and actionable intelligence to law enforcement
- A properly trained, adequately staffed and equipped counterterrorism police capacity
- A well-trained, professionally aggressive prosecution service operating within an efficient criminal justice system

When we speak of focus, we speak of priority, and from my seat this is where our focus ought to be. When this is in

"At a time when the threat to national security is manifest, as it is now because of terrorism, I suggest we should focus on dealing with the immediacy of this threat before focusing any further on the broader range of issues affecting our security."

hand, we can go shopping for sprinklers. So my answer is no.

Senator Colin Kenny

I don't think Canada's national security infrastructure is overly focused on anything at the moment. The Mounties (RCMP) are drastically underfunded. The Canadian Forces are drastically underfunded. The Canadian Security Intelligence Service (CSIS) is drastically underfunded. The list goes on.

As a result, Canadians and Canadian interests are becoming increasingly vulnerable in the context of a quickly changing world, and not just to terrorists, but to natural disasters, challenges to the country's sovereignty and territorial integrity, pandemics, industrial espionage — it's a long list.

But to get specific about whether Canada is spending too high a percentage of its security budget on terrorism, I believe the answer is no. But then I'm not a big gambler in situations in which losing a bet would be devastating.

Taking a laissez-faire approach to terrorism in the 21st century represents a reckless gamble. The whole nature of terrorism changed when a significant number of people began to make it clear that they were ready to blow themselves up to exact random acts of terrorism on innocent people in the name of a cause.

You simply can't shrug off that kind of thing and pretend that it isn't likely to happen in Canada. It will happen sooner or later, and the more lax we are in defending against it, the more likely it becomes.

To my mind, Canada's not investing sufficiently in anti-terrorist systems equates to countries like Indonesia not having invested sufficiently in tsunami warning systems. Tsunamis aren't everyday occurrences anywhere in the world, but they are a good thing to prepare for. So are terrorists.

I could tell you dozens of ways that Canadian anti-terrorist preparation is inadequate. Here are just a few. How is it that CSIS, Canada's anti-terrorist nerve centre, has fewer employees now than it had 18 years ago? How is it that passengers boarding Canadian flights can't take a penknife on board, but postal packages flow into the hold virtually uninspected? How is it that we are leaving it to 14 Mounties to defend Canada's soft underbelly — the Great Lakes?

One recent incident in Ottawa involved "geocaching," a game in which people hide packages of innocent stuff, and other people use Global Positioning devices to try and find them. In this incident, a member of the geocaching community left a "cache" — a metal cigar box filled with trinkets — attached to a light post in a vulnerable urban area. An alert citizen informed police, and the bomb squad was called in. Part of a major traffic artery and the bus transitway were shut down for four hours.

It turns out there are hundreds of packages like this scattered playfully around Ottawa, some in vulnerable spots.

Was there a public outcry against doing this? Not much. Can you imagine the outrage there would be in Tel Aviv, or Kandahar City, or Washington?

Maybe most Canadians figure the best defence against terrorism is not to get too worked up about it. Maybe. But the Indonesians are doing a lot more to prepare for the possibility of tsunamis these days. Makes sense to me.

Norman Inkster

That is a difficult question to answer. If one were to agree with the statement, one would not want to be wrong! Designing security approaches is extraordinarily challenging for authorities given the paucity of resources and the shortage of time in any given day. There will never be enough resources available to attend to all of the work that needs to be done.

With the turmoil in today's world, we could certainly not fault anyone for giving the potential criminal acts of terrorists a very high priority.

Another challenge is getting any real consensus around the definition of terrorism, all the while remembering that one person's terrorist is another person's freedom fighter. Given the misguided thinking of religious and ideological zealots, a criminal act in the name of terrorism can come from almost anywhere at any time.

We run the risk of misapplying some of our scarce resources if, by focusing on the subject of terrorism — which is not clearly defined and some say gives the actions of terrorists an air of legitimacy — we ignore what law enforcement and other security authorities must focus on: acts of crime, criminal behaviour and criminal conspiracies of which terrorist activity is but one source.

The traditional law enforcement approaches — prevent, detect, investigate — will always be the best and more effective ways to protect the public and bring suspects before the courts of law. In short, terrorist groups need to be a focus for the authorities because those groups are — by intent and often by definition — going to be involved in acts of crime.

Terrorism needs to be seen as a source of harmful criminal activity, but it is only one source. Authorities must not become so focused on the activities of terrorists that they ignore the potential for harmful criminal activity by others who, for any number of misguided reasons having nothing to do with either religion or ideology, would place a bomb on an airplane, in a crowded shopping mall or elsewhere with equally devastating results to innocent members of the public.

The challenges for authorities are about agility and balance. Be agile enough to recognize that unanticipated events will occur from unexpected sources, and keep a preventive, watchful eye for these developments. Move resources and adjust focus quickly to deal with unusual events. Get the balance right in light of the reality that there are too few people and there is too little money to do it all.

Sir Robert Peel (the founder of modern policing) said that the police are the public and the public are the police. In short, we all need to be reminded that we have an important role to play in dealing with harmful criminal activity, whether or not it is the act of a terrorist. ■

National security criminal investigations

RCMP looking to the future

By Donald Dawson
National Security Criminal Investigations, RCMP

Perhaps no other area of the RCMP has seen as many positive changes over the recent past as has National Security Criminal Investigations (NSCI).

Take the achievement of Ministerial directions on national security responsibility and accountability, national security-related arrangements and co-operation, and investigations in sensitive sectors. Add to that the implementation of RCMP-related recommendations from the Report of the Events Relating to Maher Arar, plus a complete restructuring to focus exclusively on national security.

The outcome is movement far beyond the implementation of external recommendations that look back to the past for guidance. Instead, NSCI is concentrating on the present and eyeing its future. It is moving forward in response to a constantly changing environment, explains Bob Paulson, Assistant Commissioner for NSCI.

"The threat remains real," says Paulson. "My task is to ensure that we continue to protect Canadians while ensuring we look after the people we expect to do this work."

He points to how NSCI's internal oversight of operations has been completely reformed, with its members now benefiting from a clear and concise framework that ensures strong central control and monitoring of criminal investigations by national headquarters. This includes new policy directives and new course training standards that surpass even the O'Connor Commission's recommendations. A reworked national security criminal investigators' course and other national security courses are now more widely available to national security staff. The courses also cover issues arising from the O'Connor inquiry, including RCMP and Canadian Security Intelligence Service (CSIS) mandates, information sharing, caveats on how information can be used and the role of liaison officers.

NSCI is now looking to the horizon and beyond, says Insp Scott Doran, acting director of the National Security Criminal Operations Branch.

"What we're doing now is aiming to consistently raise the bar," says Doran. "I think this embrace of change, this striving for constant improvement, is the culture we are building within NSCI."

He and other national security personnel point to significant recent successes at NSCI. In many cases the directorate has decisively surpassed its goals.

For instance, according to its most recent Departmental Performance Report, the RCMP disrupted more significant terrorist targets in 2006–2007 than originally planned and more than doubled its target of 10 new or expanded information sources or techniques that advance specific national security initiatives.

Perhaps more telling than the statistics

Driving change: the recipe for national security

More Integrated National Security Enforcement Teams (INSETs)

INSET expansion is a priority. The current INSETs in Montreal, Ottawa, Toronto and Vancouver have proven their value. Their integrated nature — bringing RCMP members together with municipal and provincial police and intelligence partners — improves co-operation and co-ordination, achieves economies of scale and reduces duplication. But national security files are being generated in many other places across Canada. Near-term plans call for the establishment of an INSET in Alberta. Further down the line, NSCI is hoping to bring INSETs to other provinces.

Engagement of critical infrastructure stakeholders

NSCI is pursuing increased stakeholder engagement through the Suspicious Incident Reporting (SIR) system, which became operational as a pilot project this spring. SIR is a secure system for reporting, sharing and analyzing information on suspicious activities that may represent terrorist planning or other serious criminal activity. The system is meant to help detect and prevent significant national security crimes before they're an imminent threat to Canadians and Canadian infrastructure.

The current pilot involves major transit operators in Toronto and Vancouver, but the intent is to eventually involve owners and operators among all critical infrastructure sectors in all parts of Canada. By facilitating the proper sharing of information on potential threats with those who need to know, the overall goal is to make Canadians, Canadian critical infrastructure and Canada as a whole safer.

More outreach leading to greater understanding

NSCI is also working to grow its outreach program, which was established in 2005. In addition to divisional outreach programs in British Columbia (B.C.), the National Capital Region and Southern Ontario, the program has shown great success at building mutual trust and understanding between the RCMP and members of communities most affected by national security operations. One of the program's components seeks to help communities counter attempts to radicalize young people. The intent is to

are the operational successes themselves — from the ongoing terror trials in Ottawa and Toronto, to a terrorist financing charge laid earlier this year in British Columbia, to the seizing this past spring of bank accounts and the Montreal headquarters of the World Tamil Movement, a group subsequently listed as a terrorist organization by the Canadian government.

"I think people are finally understanding the urgency of the situation and appreciating the threat we face, both operationally and institutionally, says Paulson. "Terrorism is a crime. The RCMP prevents, detects, disrupts and investigates terrorism and other national security offences. And, by and large, it does a darned good job."

That job includes the RCMP's commitment to integration with its partners, particularly other police forces and CSIS. Co-operation with these groups on national security matters has only improved in the recent past. Last August, the RCMP, in conjunction with other members of the Canadian Association of Chiefs of Police, adopted the Common Framework on National Security to collectively and co-operatively guide Canadian law enforcement's fight against terrorism and threats to national security. The previous year, the RCMP signed a renewed memorandum of understanding (MOU) with CSIS. The new MOU is indicative of the close working relationship built between the two agencies over the last two years.

Internally, NSCI is also working to maintain the positive momentum. Current issues include expanding the Integrated National Security Enforcement Teams (INSETs) to other divisions, increasing NSCI's engagement with critical infrastructure stakeholders, building on the success of its outreach activities, and strengthening investigations through the Office of Investigative Standards and Practices.

NSCI will face additional external scrutiny of past operations later this year. Both the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, and the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 are expected to soon submit their reports to government. But the hope among NSCI personnel is that in examining their organization's actions from years ago, the commissions will consider both the positive changes recently implemented and those that are on the way. ■

help communities build an immunity to messages that promote hatred and criminality towards others. The outreach program is also one of the many ways the RCMP is promoting its National Security Information Network and the network's 1-800-420-5805 toll-free tip line. Other ways include its website, training videos, publications and other communication products.

Office of Investigative Standards and Practices

The establishment of the Office of Investigative Standards and Practices (OISP) just this year is intended to strengthen our operations by heightening internal oversight and raising accountability with respect to national security criminal investigations across Canada. A key function of the OISP is the institution and management of a major case management (MCM) accreditation program for team commanders. These commanders will, in turn, ensure accountability, clear goals and objectives, sound planning, proper utilization of resources, and control over the speed, flow and direction of RCMP investigations.

The objective is to increase the likelihood of successful prosecutions by ensuring investigations adhere to MCM principles. The National Security OISP follows the example set by the RCMP's highly successful B.C.-based OISP and may eventually serve as the basis for the creation of a nationwide office aimed at ensuring MCM principles are closely followed in all significant investigations.

What's in a word? A lot, in the world of national security

Words make worlds, but they also break them.

That's the message Angus Smith, officer in charge of Alternative Analysis with "RCMP National Security Criminal Investigations regularly tries to convey to officers who engage the public on issues related to radicalization and criminal extremism.

Take the word jihad, for example. Smith says the word has become "almost a catchall term for extremism of any kind," but that's a harmful misnomer.

"Jihad doesn't have negative connotations in Arabic — it has positive connotations," says Smith. "It's about one's struggle in the larger social context. It's really about struggling to become a better person, to make the world a better place."

When officers use the word jihad in relation to criminal extremism, says Smith, they risk isolating the communities they're trying to help and legitimizing the extremists they're trying to hinder.

"We have to understand these types of cultural nuances," says Smith. "As an organization (we need to) understand what we're talking about."

With this cultural clarity in mind, the Ottawa RCMP national security community outreach team and its local community advisory group organized a series of Muslim–Arab cultural awareness sessions. During each session, members of the local Muslim–Arab community spend a day educating Ottawa-area officers about Islamic faith and providing advice on how to communicate in a culturally appropriate manner.

So far, 500 officers have attended the sessions. For the RCMP that's 500 more officers whose words will make worlds, not break them.

— Caroline Ross

are the operational successes themselves

from the ongoing terror trials in Ottawa and Toronto, to a terrorist financing charge laid earlier this year in British Columbia, to the seizing this past spring of bank accounts and the Montreal headquarters of the World Tamil Movement, a group subsequently listed as a terrorist organization by the Canadian government.

"I think people are finally understanding the urgency of the situation and appreciating the threat we face, both operationally and institutionally, says Paulson. "Terrorism is a crime. The RCMP prevents, detects, disrupts and investigates terrorism and other national security offences. And, by and large, it does a darned good job."

That job includes the RCMP's commitment to integration with its partners, particularly other police forces and CSIS. Co-operation with these groups on national security matters has only improved in the recent past. Last August, the RCMP, in conjunction with other members of the Canadian Association of Chiefs of Police, adopted the Common Framework on National Security to collectively and co-operatively guide Canadian law enforcement's fight against terrorism and threats to national security. The previous year, the RCMP signed a renewed memorandum of understanding (MOU) with CSIS. The new MOU is indicative of the close working relationship built between the two agencies over the last two years.

Internally, NSCI is also working to maintain the positive momentum. Current issues include expanding the Integrated National Security Enforcement Teams (INSETs) to other divisions, increasing NSCI's engagement with critical infrastructure stakeholders, building on the success of its outreach activities, and strengthening investigations through the Office of Investigative Standards and Practices.

NSCI will face additional external scrutiny of past operations later this year. Both the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, and the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 are expected to soon submit their reports to government. But the hope among NSCI personnel is that in examining their organization's actions from years ago, the commissions will consider both the positive changes recently implemented and those that are on the way. ■

help communities build an immunity to messages that promote hatred and criminality towards others. The outreach program is also one of the many ways the RCMP is promoting its National Security Information Network and the network's 1-800-420-5805 toll-free tip line. Other ways include its website, training videos, publications and other communication products.

Office of Investigative Standards and Practices

The establishment of the Office of Investigative Standards and Practices (OISP) just this year is intended to strengthen our operations by heightening internal oversight and raising accountability with respect to national security criminal investigations across Canada. A key function of the OISP is the institution and management of a major case management (MCM) accreditation program for team commanders. These commanders will, in turn, ensure accountability, clear goals and objectives, sound planning, proper utilization of resources, and control over the speed, flow and direction of RCMP investigations.

The objective is to increase the likelihood of successful prosecutions by ensuring investigations adhere to MCM principles. The National Security OISP follows the example set by the RCMP's highly successful B.C.-based OISP and may eventually serve as the basis for the creation of a nationwide office aimed at ensuring MCM principles are closely followed in all significant investigations.

What's in a word? A lot, in the world of national security

Words make worlds, but they also break them

That's the message Angus Smith, officer in charge of Alternative Analysis with RCMP National Security Criminal Investigations, regularly tries to convey to officers who engage the public on issues related to radicalization and criminal extremism.

Take the word jihad, for example. Smith says the word has become "almost a catchall term for extremism of any kind," but that's a harmful misnomer.

"Jihad doesn't have negative connotations in Arabic — it has positive connotations," says Smith. "It's about one's struggle in the larger social context. It's really about struggling to become a better person, to make the world a better place."

When officers use the word jihad in relation to criminal extremism, says Smith, they risk isolating the communities they're trying to help and legitimizing the extremists they're trying to hinder.

"We have to understand these types of cultural nuances," says Smith. "As an organization, (we need to) understand what we're talking about."

With this cultural clarity in mind, the Ottawa RCMP national security community outreach team and its local community advisory group organized a series of Muslim–Arab cultural awareness sessions. During each session, members of the local Muslim–Arab community spend a day educating Ottawa-area officers about Islamic faith and providing advice on how to communicate in a culturally appropriate manner.

So far, 500 officers have attended the sessions. For the RCMP, that's 500 more officers whose words will make worlds, not break them.

– Caroline Ross

The continuum of corruption

Reducing security threats from abroad

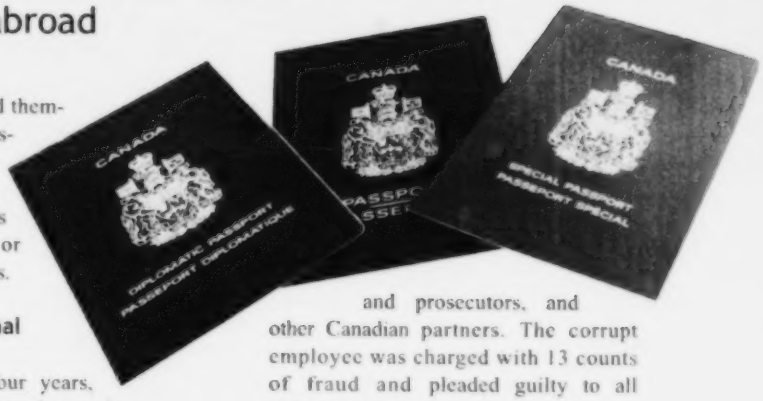
By Sgt Robert Cloutier
Senior investigator
RCMP Immigration and Passport
Special Investigation Section

National security is a well-established priority for the RCMP. This commitment is evident through frameworks like the Integrated National Security Enforcement Teams operated by National Security Criminal Investigations. But another section of the RCMP also plays an integral role in protecting Canadian national security: the Immigration and Passport Special Investigation Section (IPSIS).

Based in Ottawa, IPSIS is a unique investigative team, exclusive of its kind. Members work in concert with partner government agencies such as the Department of Foreign Affairs and International Trade, Citizenship and Immigration Canada and Passport Canada to identify and investigate cases of malfeasance in Canadian High Commissions and Canadian Embassies abroad. The unit is primarily responsible for investigating immigration fraud and corruption of government officials that impact the integrity of the Canadian immigration system.

What does this have to do with national security? A lot, when you consider the integrity of our borders. Foreign criminals who smuggle or traffic in humans, weapons or drugs — or wish to attempt a terrorist act — ultimately need to gain entry to Canada, and for that, they need official travel documents. These unsavoury individuals often seek the assistance of employees in Canadian diplomatic missions. That is precisely where the continuum of corruption begins.

Outsiders usually start by subtly befriending mission employees, then asking for discreet favours that compromise employee integrity — favours like issuing illegal visas or travel documents. Employees who agree to these "favours" eventually find themselves in an inescapable position, and one that often leads to dismissal or criminal charges.



Investigational success

In the past four years, IPSIS has conducted several international investigations involving mission employees who participated in illicit activities related to visa or passport issuance. IPSIS investigators travelled to Guyana, Poland, India, Pakistan and Turkey, to name just a few countries implicated in the investigations.

In fall 2004, IPSIS investigators searched the office of an individual responsible for issuing Canadian passports at the High Commission of Canada in Georgetown, Guyana. The investigators encountered a disturbing scene: hundreds of passport photographs strewn on the floor, and an inventory of expired but authentic Canadian passport documents that were being used to falsify passport applications for Guyanese nationals wanting to exit the country.

A well-known Guyanese human smuggler had planned his strategy well, convincing a woman who worked at the High Commission that he loved her. The woman did him one favour by helping him obtain an illegal Canadian passport for a friend. Then came the second request, the third, and so forth. Eventually, 55 Canadian passports were forged for the purposes of smuggling people into Canada. Some passports were sold on the street for as much as US$14,000.

The operation continued for several months until it was dismantled by IPSIS, in co-operation with Guyanese authorities and prosecutors, and other Canadian partners. The corrupt employee was charged with 13 counts of fraud and pleaded guilty to all charges.

Overcoming challenges

IPSIS investigators face several challenges in their work, including language barriers, limitations on information gathering and sharing due to human rights issues, physical security in foreign countries, and legislative gaps that make it difficult to carry out investigations thoroughly.

In the face of such hurdles, the team continuously seeks innovative methods of investigating abroad. For example, during a recent investigation, IPSIS requested assistance from a truth verification technician (polygraph operator) — an action that had never before been taken in an investigation of this type.

IPSIS is also working to increase awareness of its mandate, in hopes of increasing the flow of information and intelligence that could factor into investigations. The team gives presentations to Citizen and Immigration Canada, Passport Canada, the Canada Border Services Agency and RCMP foreign liaison officers, with a view to developing mutual goals in protecting our nation's security.

IPSIS is also building a working group with other countries that face the same contentious issues. Knowledge is the key to preventing future attacks on the integrity of Canadian travel documents and borders, and to stemming the corruption that occurs when greed and opportunity intersect. ■

Youth engagement on national security

Countering misconceptions and building trust

By Caroline Ross

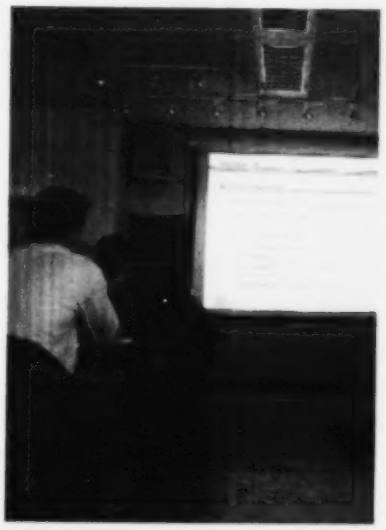
Youth: they're the leaders of tomorrow. Unfortunately, a small percentage may also become the criminal extremists of today.

"Historically, when you look at (individuals involved in) criminal extremism, you're looking at the ages between 14 and 30," says Sgt Raj Jande, RCMP National Security Outreach Co-ordinator. "Young people are open to ideas, they are full of gusto, and they are looking for their identity."

Many youth want to influence change in society, but their dedication to a cause could be manipulated. That's why youth outreach is a growing priority for the RCMP National Security Criminal Investigations branch.

Countering misconceptions

When Dahlia Nawwar began co-ordinating the new RCMP National Security Youth Outreach Program in 2005, she quickly realized that young people lacked impartial information on national security issues.



Guylain Ouellette

Students in Ottawa listen to a presentation by the RCMP National Security Youth Outreach Program.

"There are a lot of misconceptions out there," says Nawwar, citing confusion between security certificates and the Anti-Terrorism Act as just one example. Nawwar attributes many of the misconceptions to media biases, combined with the fact that the RCMP and federal agencies weren't contributing information to the public dialogue on national security issues.

"There was a gap," says Nawwar. "There was a need for educational resources on national security within the Canadian context, (so that) young Canadians (have) balanced and objective information."

To help fill the void, Nawwar spearheaded the creation of a fact sheet and presentation materials that clearly define national security, terrorism, related legislation and related RCMP responsibilities from a Canadian perspective. The materials are available to young people through RCMP youth officers and national security outreach initiatives.

But police can't just talk at youth, says Nawwar, they must also listen. The outreach unit holds regular meetings with its Ottawa-based youth steering committee.

In spring 2008, the unit also partnered with the Government of Canada's Canadian Youth Connection Forum to hold an online survey and discussion called "Youth: Be Heard on National Security."

"It's really important to have that two-way conversation," says Nawwar. "Youth have some very insightful perspectives that we really should listen to."

Building trust

One of the biggest challenges to national security outreach is establishing trust within vulnerable communities, says Cst Mohammad Beyhaghi. Beyhaghi co-ordinates RCMP national security youth outreach initiatives in British Columbia (B.C.). He encountered the challenge first-hand when he began engaging Vancouver's Muslim community in early 2007.

"(Some community members) have this misconception that if the police come in — especially from national security — they come to collect information or get community members to spy on other community members," says Beyhaghi. "(As police, we) have to convince them that we are here to work with (them)."

After six months of meetings and consultations, Beyhaghi formed the B.C. RCMP National Security Youth Advisory Council, then gave the group of 15 young Muslims the reins to organize a major Muslim youth conference on radicalization and criminal extremism. The March 2008 event — the first of its kind in Canada — attracted 130 youth and included a parallel conference for parents.

"It was a ground-breaking event, indeed," says Sana Siddiqui, a member of the youth advisory council. "It was a recognition that solutions to community-based problems can come from the community."

B.C. RCMP outreach initiatives also extend to Muslim children aged six to 12. The outreach team runs a Junior Police Academy program that allows Muslim kids to interact with police officers in a fun learning environment. The goal is to build bridges with kids at an early age, before they reach those crucial teens and twenties.

While RCMP national security youth outreach initiatives do face some operational obstacles — like a paucity of dedicated youth outreach positions nationwide — current initiatives provide a solid foundation for growth.

They also prove that police and youth can work together on issues of concern.

"I feel that the trust has gone up," says Beyhaghi in B.C. "It doesn't feel false." ■

The London bombings, through the eyes of the survivors

Journalist provides first-hand account

*A bang, a jolt, darkness, then terror. That's what Canadian journalist Peter Zimonjic experienced on July 7, 2005, when a terrorist bomb blasted through the London Underground subway train next to the one in which he was riding. Minutes after the blast, Zimonjic crossed into the bombed train to offer assistance. Weeks later, he launched a victim-support website. This year, he released a book chronicling the London bombings through the eyes of dozens of survivors (*Into the Darkness: An Account of 7/7, *Vintage Originals, 2008). Zimonjic talks with the* Gazette*'s Caroline Ross about his website, his book and the July 7 emergency response.*

Brigitte Bouvrette

Peter Zimonjic survived the 2005 London transit bombings then wrote a book chronicling events at ground level. He praises some aspects of the emergency response, but says there are definitely learning opportunities.

What has been the response to your website (www.londonrecovers.com)?

The first year, I had about 200 users. I would say most people were motivated by a desire to find out if someone they met on that day was OK. Another motivation was to discuss the way they felt about the day itself, to get (informal) psychological help. Since the first anniversary (of the bombings), people are using the site less, which I think is an indication that people are healing.

Did you have any contact with law enforcement through the website?

I did meet some police officers who were involved in the day. Usually they contacted me looking for some way to get psychological help without having to go through their workplace, because they felt there was a culture of looking down on people who need counselling for experiencing something like that. I met police officers who had not even told their own families that they were involved that day. They often needed a bit of reassurance that others were thinking and feeling the same thing, and they could find that (reassurance) on the website.

What did you learn about survivors' interactions with authorities after the attacks?

Everyone I talked to seemed quite pleased with the way the police used family liaison officers to help families keep in touch with the events surrounding their family members. City police did a very good job of keeping all of us involved every step of the way. I still get letters updating me as to what is happening with various court cases or inquests. Further government support through the 7 July Assistance Centre (which offers therapeutic and information resources), was very useful, very swiftly set up and very well maintained afterwards.

What lessons can authorities take from the day's events?

It took an hour before any emergency services could get down (into the tunnels). I realize that there are certain safety protocols involved in not rushing into a scene that's considered to be unsafe, but I think there could be some thought given to sending a scout down, with some protective gear, to do a very early-on assessment of the situation. I know that people died in the tunnel waiting for help.

I also think it would be useful to require potential terrorist targets like underground subway trains to carry first aid equipment and emergency lighting. It's very difficult to save someone's life if both their legs have been blown off and you have absolutely no medical equipment, and it's dark. There were stretchers on the Underground train in London, but nobody knew where they were, and as a result, they couldn't be used to get people out.

Why should people read your book?

I think it's important to remind ourselves of the human cost of terrorism. Often the argument after a terrorist attack quickly shifts to government policy or civil liberties. In the media, victims often become advocates for positions one way or the other. I think it's important to sweep that aside and remind ourselves of what happened — the human cost of things — and to stay focused on that sort of human tragedy. ■

> **"I met police officers who had not even told their own families that they were involved that day. They often needed a bit of reassurance that others were thinking and feeling the same thing."**

The Canadian Air Carrier Protective Program

By Marc-André Gauthier

The Canadian Air Carrier Protective Program (CACPP) evolved in the aftermath of the September 11, 2001, terrorist attacks on the United States. RCMP air marshals — known as Aircraft Protective Officers or, internationally, as In-Flight Security Officers (IFSOs) — started blending in with passengers on all Canadian flights to Washington, D.C., in 2002. They are now tasked to other routes as well.

IFSOs provide a unique protective policing service on board Canadian registered commercial aircraft. These officers are specialized, covert operatives who are strategically deployed to physically intervene in the event that an aircraft becomes at risk of takeover by unauthorized person(s). In addition, IFSOs gather information on any criminal or terrorist activity within the civil aviation environment. For national security reasons, the exact flights and routes protected by the CACPP are carefully guarded secrets. However, the CACPP deploys on a national, transborder and international basis.

In October 2007, RCMP Supt Alphonse MacNeil, the officer in charge of the CACPP, told the Air India Inquiry that the public should take comfort in the fact that RCMP IFSOs are deployed on commercial passenger flights. MacNeil explained that the specialized plainclothes officers are assigned to selected commercial passenger flights according to a threat-risk assessment process.

He said that selected officers train at an undisclosed location, where they can practise scenarios in a commercial aircraft environment. Once the IFSOs have completed this very intensive and highly specialized training, they are assigned to flights according to a "threat matrix."

When questions arose about whether the presence of armed IFSOs on board commercial passenger flights could pose a risk to the security of jetliners, MacNeil explained that the intense training that Canadian IFSOs receive mitigates that risk. He emphasized that firearms would only be used as a last resort.

"We don't immediately spring to the use of a firearm," said MacNeil. "Our people are well trained in . . . the use of hand-to-hand combat and other procedures that are at their disposal. If one of our (IFSOs) is going to engage . . . a firearm, things have deteriorated very, very badly on that flight and they would actually believe that the aircraft is in danger of being taken over or the integrity of the aircraft is in serious risk," said MacNeil.

The program is necessarily covert to protect the identity of the officers and their operations. However, pilots and flight attendants are informed of the presence of IFSOs. Many measures are in place to protect Canadian airline passengers from terrorist or criminal threats, and the CACPP is a critical layer in the multi-tiered approach to aviation safety and security. IFSOs are the last line of defence in the civil aviation security system.

The CACPP focuses its sights not only on terrorist activity, but also on criminal activity within the airport environment itself. The program houses an effective intelligence program that employs IFSOs in an intelligence-gathering and surveillance capacity. This broad mandate allows observation and analysis performed by the covert operatives to be fed into the RCMP's greater national intelligence system. Furthermore, the operatives work closely with numerous RCMP sections and partner agencies in the airport environment.

The CACPP has evolved into an integral component of one of the most secure aviation systems in the world. It has been extensively involved in international IFSO programs, and agencies around the globe have requested its expertise. The program has provided complete IFSO training and program development for several foreign countries, with others waiting to receive this specialized training.

At the Air India Inquiry, the inquiry's Commissioner, John Major, suggested that the general public might feel safer if people knew more about the program. MacNeil agreed, but explained that it is difficult to publicize the program when so many details must remain secret for national security reasons.

Balancing the need to protect the integrity of the program with the need to create public awareness is a challenge that the CACPP is prepared to meet. With a comprehensive package being developed to achieve this goal, the Canadian public will become increasingly aware of this superbly trained tactical unit and the unique protective services it offers for the protection of Canadians and Canadian interests at home and abroad. ■

Developing an all-hazards risk assessment model

By Alain Goudreau, M.Sc., P.Eng.
Centre for Security Science
Defence R&D Canada

In the fall of 2006, the RCMP Critical Incident Preparedness and Response initiative published an integrated risk management report identifying the need for a common all-hazards risk assessment (AHRA) picture for the Government of Canada. The Department of National Defence (DND) Canada Command also identified this need in its survey of the Canadian operational environment.

In December 2006, a federal-level Intelligence Experts Group (IEG) on Domestic Security was established to pursue the development of an AHRA. The IEG, which at the outset represented exclusively federal departments and agencies with mandated intelligence capacities, grew to include some 20 federal departments and agencies that share responsibility for assessing and monitoring various risks to the safety and security of Canadians.

The IEG engaged the Centre for Security Science, one of seven research centres of Defence R&D Canada (the research and development arm of DND), to assist in managing the IEG study on AHRA, and to co-ordinate the study's scientific content.

This article outlines the nature of the study and the progress thus far.

The AHRA study

The AHRA study is a three-year project to research, conceive and test a common framework for conducting all-hazards risk assessments across the federal government. A common risk picture could provide invaluable information to assist decision-makers in evaluating Canada's ability to prepare for — and respond to — threats and hazards, be they from terrorists, criminals, accidents or natural disasters.

The study will also explore the broader impact of a robust, established risk assessment process on decision-making in the safety and security domain. As well, it will examine the ability to seek and share expertise as a capacity in government, and make recommendations to support the implementation of such expertise over the long term.

The study promotes these essential steps for conceiving and implementing a risk assessment framework:

- State the problem clearly. What is the objective?
- Formulate the approach. Choose the most applicable method(s).
- Collect data and/or interview experts. Consider the data source, reliability, etc.
- Build the model and establish a baseline for test results.
- Conduct a sensitivity analysis to test data sets for suspect or erroneous results.
- Record results.
- Document the model.

As work to establish the common framework progresses, the study team is addressing several related challenges.

Back to risk basics

Terminology represented the first big challenge the study team faced. The term "risk" conveys different meanings to different people, disciplines and communities. The challenge of reconciling definitions became even more complex when terms associated with risk management were introduced. "Risk perception" emerged as a fundamental concept to be explored further. The term "all-hazards risk" also conveyed different meanings, with no evidence of an accepted standard definition.

The study team tackled the terminology issue by developing a lexicon of risk terms to establish a common language. The team also developed a taxonomy (classification system) of risk events. The taxonomy was useful in communicating the meaning of all-hazards risk, and it highlighted the value of using classification systems to organize or map other aspects of risk, such as threats, hazards, vulnerabilities and even consequences.

The study team encountered a further challenge in applying the traditional definition of risk as a function of probability and consequence to various domains where the concept didn't seem to fit. The term "probability" also conveyed a meaning that was difficult to adopt, especially for the risk domains associated with randomness, like terrorism.

The team identified a need to express risk based on a clear understanding of what elements or components, such as intent and opportunity, make up the term. As such, the team chose a more universal and widely accepted risk assessment principle:

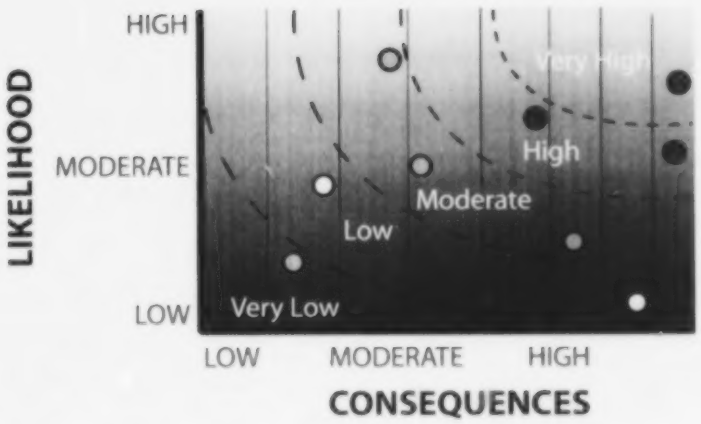
$$\text{risk manitude} = \text{likelihood of occurance} \times \text{magnitude of consequence}$$

This equation for risk can be further broken down into its components or elements. This simple process gives a better understanding of the various types of data necessary to convey the magnitude of a risk, including attributes such as reliability and time dependence.

Why is risk so fundamental?

In Canada, all levels of government — federal, provincial/territorial and municipal — share the responsibility of protecting Canadians and Canadian society. Preparedness at the national level depends on synchronized efforts among the many departments and agencies that share public safety and security functions within each jurisdiction.

For practical reasons, any attempt to



formalize an overarching risk model needs to respect existing structures of ownership and responsibility in managing risks. For example, in Canada, public safety and security functions cross jurisdictional boundaries based on the severity of the consequences of the realized risk event. This adds to the complexity of planning and managing even single emergencies that escalate across jurisdictions and organizational boundaries.

All-hazards planning is further challenged by the lack of a coherent picture of the relative severity of the risks associated with various threats and hazards. Such a picture is important, however. The all-hazards risk classification (taxonomy) approach advocated by the AHRA study supports harmonized planning across levels of government and different organizations.

Communicating and visualizing risks

Communicating the results of a risk assessment without over-emphasizing or minimizing criticality or confidence in the results remains a real challenge. One may think of a scenario where senior officials — having to make critical decisions — are presented with a risk picture composed of many types of data of various levels of accuracy and reliability. What may seem a simple exercise in ranking risk may in some cases create an erroneous picture if caveats such as data reliability are not recognized or communicated. To improve the accuracy of assessments, the AHRA study will look at applying existing techniques and technologies for modelling, analyzing and visualizing complex and abundant data — including geomatic applications and visualization tools — to the common risk picture.

The team's attempts at visualizing risks and building on the risk event taxonomy resulted in the development of a measure called "risk volume." Risk volume is determined by the magnitude of the risk components, such as probability, vulnerability and consequence. Attempting to mitigate or affect any one component changes the risk volume. This approach may be useful in conveying the impact of risk mitigation and management options.

Another approach is to look at risk and its component taxonomies in terms of three or more domains: human and social, physical, and environmental. It can be said that every risk or its components fall within one of these domains or at their intersection. The choice of domains remains a matter of preference for the practitioner. By mapping risks and their components in this way, one gets a sense of the distribution of risks across domains. Combining this information with other elements like capabilities available (a bomb squad, for instance), capability investments or operational plans produces a more detailed risk picture.

Many organizations have adapted a two-dimensional graph to map risks and their magnitude (see illustration). In this case, the hash lines denote the thresholds for the various risk levels. The hash lines are established as a risk management decision, and their location often reflects the risk tolerance or operational preparedness of an organization.

Challenges ahead

To date, the AHRA study has served to highlight the difficulty in implementing a robust risk regime in everyday decision-making, be it for short-term actions or long-term planning. Organizational decision-making is challenged more and more by the push towards risk management regimes. The lack of a robust understanding of risk fundamentals across an organization will jeopardize the implementation of a sound risk management regime.

The level of detail needed by an organization will vary greatly depending on the level (tactical, operational, strategic or local, regional provincial or national) and speed of influence (from policy to capability owner). Processes for tracking and auditing risks must be rigorous. As such, organizations should consider dealing with terminology at the outset. They should also consider structuring the risk problem through taxonomies that facilitate the development of criteria to be measured. For each criterion, an appropriate metric should be adopted. Consistency in applying the taxonomy, the criteria and the metrics will be key to a robust risk assessment.

Communicating risk and uncertainty remains a real challenge. The time component or life aspect of risk — and its effect on individual components of risk — requires consideration, as does the notion of multiple risk assessments for different time horizons. The risk picture becomes more speculative as we look to the future.

The study team expects to conclude its work and report its findings in 2010-2011. ■

Narrowcasting: The trend in online terrorism

Prof. Gabriel Weimann, PhD
University of Haifa, Israel

The Internet is the ideal instrument of communication for modern terrorists: it is decentralized, it cannot be subjected to control or restriction, it allows access to anyone who wants it, and it provides almost perfect anonymity. These advantages have not gone unnoticed by terrorist organizations.

Today, all terrorist groups, large or small, have their own websites. They use this medium to spread propaganda, raise funds, launder money, recruit and train members, communicate and conspire, and plan and launch attacks.

Al-Qaida, for example, is now operating approximately 5,600 websites, with 900 new sites appearing each year. Along with websites, modern terrorists also use e-mail, chat rooms, e-groups, forums, virtual message boards, YouTube and even Google Earth.

This article is based on a decade-long project of monitoring and analyzing terrorist presence on the Internet. One of the recent trends emerging from the analysis is "narrowcasting," whereby Internet-savvy terrorists target specific sub-populations. Instead of "broadcasting" — that is, trying to appeal to as broad an audience as possible with a single message — terrorist groups are getting audience-specific. This trend employs the modern marketing and advertising tactics used in the commercial world, and it can be illustrated with several examples from our archive of terrorist websites.

Targeting children

The Internet is very popular among children and young people who use it for entertainment, communication and learning. Terrorists are aware of this and are increasingly using the Internet to target children as the next generation of recruits and supporters.

One Hamas website, *al-Fateh* ("The Conqueror"), which releases a new edition every other week, is geared towards children. Among its attractive graphics, drawings, children's songs, stories and texts written by children themselves, this seemingly innocent site includes a link to the official Hamas website and posts messages promoting suicide terrorism.

For example, the site posted a picture of the decapitated head of young Zaynab Abu Salem, a female suicide bomber who, on September 22, 2004, detonated an explosive belt in Jerusalem, killing two policemen and wounding 17 civilians. The text accompanying this horrible image praises the act, arguing that Zaynab Abu Salem is now in paradise — a *shaheeda* (martyr) like her male comrades: "Her head was severed from her pure body and her headscarf remained to decorate (her face). Your place is in heaven in the upper skies, oh, Zaynab, sister (raised to the status of heroic) men."

Terrorists are also aware of children's fascination with computer games. Several terrorist groups try to attract children by offering free online games that turn out to be instruments of radicalization and training. One such game, called "Quest for (U.S. President George W.) Bush" or "Night of Bush Capturing," was released by the Global Islamic Media Front, a media outlet of al-Qaida, in September 2006. Players armed with rifles, shotguns or grenade launchers navigate various missions, with the ultimate goal of killing President Bush.

Another example is Hezbollah's online game "Special Force," in which players become warriors in a 3D terrorist campaign against Israel. Available in Arabic, English, French and Farsi, the violent game features a training mode that allows participants to practise their shooting skills on former Israeli Prime Minister Ariel Sharon and other Israeli political and military figures. Players with high scores earn special certificates signed by Hezbollah leader Sayyed Hassan Nasrallah. In August 2007, Hezbollah produced a new version of the game, "Special Force 2," based on the 2006 Lebanon War between Hezbollah and Israel.

The Internet is also used for child recruitment and training. In February 2008, the American army uncovered an online video during a raid in Iraq's Diyala province. The video depicts children in ski masks kidnapping a grown man on a bicycle, sitting in a circle around firearms singing al-Qaida songs, and storming a room with bound adult hostages, waving guns at their heads.

Jonathan Evans, head of the British security service MI5, recently said that Muslim children as young as 15 are being recruited by al-Qaida to wage "a deliberate campaign of terror." Evans warned that Islamists were "radicalizing, indoctrinating and grooming young, vulnerable people to carry out acts of terrorism." The Internet has clearly become one of the

Along with websites, modern terrorists also use e-mail, chat rooms, e-groups, forums, virtual message boards, YouTube and even Google Earth.

most efficient instruments for targeting these young audiences.

Targeting women

The ninth issue of *Sawt al-Jihad* (Voice of Jihad), al-Qaida's online magazine, was the first in a series of women-oriented postings. Published in January 2004, the issue included a special section for women and attempted to recruit women for terrorist attacks.

One article, "Um Hamza, an Example for the Woman Holy Warrior," is the story of a female martyr as told by her husband: "Um Hamza was very happy whenever she heard about a martyrdom operation carried out by a woman, whether it was in Palestine or Chechnya. She used to cry because she wanted a martyrdom operation against the Christians in the Arabian Peninsula."

In late 2004, al-Qaida launched an online women's magazine called *al-Khansa*, named after a seventh-century Islamic poetess who wrote eulogies for Muslims who died while fighting the "infidels." The website gives women advice on raising children to carry on the jihad, using first aid to treat family members injured in combat, and preparing to fight through physical training.

The main goal of the magazine seems to be to teach Islamist wives how to support their husbands in the violent war against the non-Muslim world. One of the magazine's first articles reads: "The blood of our husbands and the body parts of our children are our sacrificial offering."

On March 6, 2008, al-Sahab, the media production branch of al-Qaida, updated the Islamist website *al-Ikhlas* to include an audio message from Sheikh Mustafa Abu al-Yazid, the al-Qaida commander in Afghanistan. The message is titled "They Lied and Now (it is Time for) Combat." In it, al-Yazid stresses the importance of jihad and appeals to parents "not to be an obstacle between their sons and Paradise . . . since our religion is more expensive than our souls . . . and since (one's willingness) to sacrifice (one's) children for the sake of Allah is a clear sign of (one's) righteousness." Al-Yazid also calls upon wives not to stand in their husbands' way to Paradise, saying: "A righteous wife who loves her husband is one who wishes for him to enter Paradise . . . and who says to him . . . 'Take my gold and property and wage jihad for the sake of Allah . . . and we shall meet in Paradise, Allah willing . . . "

Terrorists are fine-tuning their appeals and sharpening their messages according to narrowly defined sub-populations.

A series of messages regarding Muslim women and their role in supporting jihad and its war on the West have also emerged on jihadist forums. One document, titled "What Do the *Mujahideen* (Muslims who struggle) Want from a Muslim Woman?" was written by Abu Omar Abdul Bar, a leading Muslim writer. Abu Omar charges that the war launched by the West against Islam is not limited to direct military action, but also seeks to affect changes in economic, social and character levels. In this regard, he believes that the enemy is trying to alienate Muslim women within their community and provoke them against Muslim society. Contrary to the Western desire to make women a "cheap commodity," this message advocates the role of women as mujahideen, citing various examples of female mujahideen in Muslim history. Abu Omar writes that a Muslim woman should support the mujahideen, feed her sons "gunpowder with milk" and raise them in the spirit of jihad.

Many of these female-oriented websites also cite various *fatwas* (religious interpretations of Islamic law) on jihad and martyrdom, and urge women to take an active part in jihad — or at least to support its fighters. In the *al-Hesbah* online forum, a female writer named Umm Hamza al-Shahid posted a message entitled "Secure Yourself a Chandelier under the Throne (in Paradise)," in which she encouraged Muslim women to carry out suicide bombings. The posting includes this call: "Sister, do you fear the horror of death and the agony of dying? . . . Don't you wish for such an end — an easy transition from this world to Paradise, without pain or agony . . . . Since death is inevitable, why should we not leave this transient (world) in our best capacity, (that is) as martyrs?"

These are only a few of the many online messages, but the trend is clear: terrorists are fine-tuning their appeals and sharpening their messages according to narrowly defined sub-populations. Advanced marketing theory and research suggest that sophisticated persuasion is more likely to succeed when the medium, the stimuli, the appeals and the graphics are tailored to the specific receivers. It appears that modern terrorists have learned how to apply narrowcasting to their online campaigns. ■

Gabriel Weimann, PhD, is a professor of communication at the University of Haifa, Israel, and at the School of International Service, American University, Washington, D.C. He was a senior fellow at the United States Institute of Peace. Weimann has written widely on modern terrorism, political campaigns and the mass media. This report distills some of the findings from an ongoing, 10-year study of terrorists' use of the Internet. His findings were reported in numerous publications including his book, Terror on the Internet: The New Arena, the New Challenges *(United States Institute of Peace, 2006).*

A look at terrorist behaviour

How they prepare, where they strike

By Brent Smith, PhD
Terrorism Research Center (TRC)
Fulbright College
University of Arkansas

Timothy McVeigh (Oklahoma bomber), the Sept. 11 hijackers and Eric Rudolph (Olympic Park bomber) all had something in common — they selected targets hundreds of miles from where they lived. McVeigh wandered the Midwest living as a transient before making his bomb in Herington, Kan., and driving 250 miles (400 kilometres) south to blast the Alfred P. Murrah Federal Building in Oklahoma City. The Sept. 11 hijackers travelled hundreds of miles to their targets. And Rudolph drove nearly 300 miles (483 kilometres) from Murphy, N.C., to bomb an abortion clinic in Birmingham, Ala.

For local police departments searching for ways to stop terrorist acts before they occur, this does not bring much comfort. When looking at these attacks, officers might get the impression that there is not much they can do about terrorism other than improving physical security at high-risk targets.

But were these infamous terrorists typical?

Although we know a great deal about the behaviour of traditional criminals, little information has been available about terrorists. Are they much different from conventional criminals, who tend to commit their crimes close to home? Research has shown that traditional criminals are spontaneous, but terrorists seem to go to great lengths preparing for their attacks — and may commit other crimes while doing so.

The National Institute of Justice (NIJ) launched a series of projects to explore patterns of terrorist behaviour. In the first of these projects, a panel of experts was assembled to examine 60 case studies involving terrorist incidents in the U.S. during the past 25 years. These cases involved the four major types of U.S. terrorist groups: left wing, right wing, single issue and international. The panel — including this author — looked at the homes of the terrorists, the locations of planning and preparation, and the sites of the terrorist incidents to discover whether any patterns emerged.

What the panel learned was intriguing: the cases of McVeigh, the Sept. 11 hijackers and Rudolph are actually unusual. In fact, most terrorists live close to their selected targets and engage in a great deal of preparation — some over the course of months or even years — that has the potential of coming to the attention of local law enforcement.

The panel studied the following incidents:

- Ten attacks by international groups that involved 93 preparatory acts
- Fourteen attacks by right-wing groups that involved 55 preparator acts
- Twenty-nine attacks by environmental groups that involved 80 preparatory acts
- Six attacks by left-wing groups that involved eight preparatory acts

Almost half (44 per cent) of all terrorists examined lived within 30 miles (48 kilometres) of their targets. But when the types of terrorist groups are examined separately, the findings are much different.

Terrorists think globally but act locally

International terrorists lived relatively near their targets, whereas right-wing terrorists lived in rural areas but selected targets reflecting the "pollutants of urban life" in nearby cities.

Terrorists most commonly prepared for their attacks with surveillance and intelligence gathering, robberies and thefts to raise funding for the group, weapons violations, and bomb manufacturing. Again, most of these behaviors took place relatively near their homes, which, in turn, were close to the targets.

Terrorists may stay close to home because of new immigration status, lack of transportation, lack of knowledge of the urban landscape or a desire to avoid attention. Among single-issue terrorists in particular, 71 per cent of the preparatory

acts occurred within 12 miles (19 kilometres) and 92 per cent within 28 miles (45 kilometres) of the target. This finding may also be attributed to the use of "unco-ordinated violence" tactics by these environmental and anti-abortion extremists, which often results in local targeting by "lone wolves" sympathetic to the cause.

A separate follow-up NIJ project that analyzed the distance between more than 250 environmental and international terrorists' homes and their targets confirmed the earlier preliminary findings that their spatial patterns are fairly similar. The analysis found that about half of the environmental terrorists and nearly three-fifths of the international terrorists lived within 30 miles (48 kilometres) of their targets. Sixty-five per cent of the environmental terrorists and 59 per cent of the international terrorists prepared for their attacks within 30 miles (48 kilometres) of their target sites.

Although the terrorists studied committed most of their preparatory offenses near their homes, they conducted robberies, burglaries and thefts much farther away — an average of 429 miles (690 kilometres) from home. This suggests that most environmental and international terrorists live near the selected target and conduct surveillance and other general preparation near their homes and the eventual location of the attack. However, major crimes to procure funding for the group — like thefts, robberies and burglaries — are intentionally committed many miles away to avoid drawing attention to the group's location and target.

The terrorist's timepiece

We found that preparations generally began less than six months before the attack and ended with a flurry of actions a day or so before. This pattern varied by group type. Single-issue and right-wing terrorists engaged in substantially less preparatory crime over a shorter period — once again, most likely reflecting the use of "leaderless resistance" and lone-wolf strategies. The planning cycle of international terrorists tended to be longer.

In our follow-up study, we took a closer look at the specific patterns of international and environmental terrorists by placing the preparations for all incidents on a time line. For instance, we examined the 21 incidents attributed to the environmental terrorist group known as "The Family," which was responsible for the Vail, Colo., ski resort arson in 1998 and many attacks against Forest Service and Bureau of Land Management buildings from 1996 to 2000.

The Family consisted of at least 16 people. The group's actions were more spontaneous than other environmental cases, with a short preparation period and little extended planning. Eighty-five per cent of their known preparation activities occurred within six days of the planned attack. An explosive device was assembled at the staging area a day or so before the incident and then delivered to the target. Participants usually returned to the staging area to destroy any evidence.

International terrorists, on the other hand, engaged in nearly three times as many preparatory acts per incident as their environmental counterparts. This may be due to the larger number of people usually involved in international incidents, the size and scope of the planned incident or simply a longer planning cycle.

Comparing the 10 international terrorist incidents that occurred on American soil, we found that the average planning cycle for international terrorists was 92 days, as opposed to 14 days for environmental terrorists. However, averages can be misleading because of significant outliers, such as the multi-year planning cycle of the Islamic extremists seeking to destroy New York City landmarks in the mid-1990s. Whereas environmental terrorists committed an overwhelming majority of their preparatory activities in the week before the incident, international terrorists took up to six months to prepare.

Whereas environmental terrorists committed an overwhelming majority of their preparatory activities in the week before the incident, international terrorists took up to six months to prepare.

Arming police with knowledge

For law enforcement agencies, the implications of these patterns are significant. Committing an act of terrorism will usually involve local preparations. Although much of this conduct will not necessarily be criminal, early intelligence may give law enforcement the opportunity to stop the terrorists before an incident occurs.

Knowledge of the threat — for example, understanding how long environmental or international terrorists prepare for their attacks — will affect the manner in which local officials respond. Identifying preparatory actions by environmental extremists may signal that an attack is imminent, whereas similar behaviour by an international group might suggest that an attack is still several months away.

Understanding that most terrorists act locally can be important to know as investigative agencies seek to prevent terrorism and arrest perpetrators. These local patterns may be used by agencies to more efficiently patrol known, high-risk target areas and gather intelligence on suspected actions within a specific distance from potential targets.

As we continue to deepen our understanding of the relationship among the location of the terrorist's home, terrorist preparation activities and the target, this growing knowledge should help officers prevent and respond to attacks. ■

This article is reprinted from the *NIJ Journal* (No. 260, July 2008) courtesy of the U.S. Department of Justice.

Brent Smith is a professor of sociology and criminal justice at the University of Arkansas. A student of terrorism for nearly 30 years, he created the American Terrorism Study in 1988 with assistance from the FBI. Smith currently serves as director of the Terrorism Research Center (TRC) in the Fulbright College at the University of Arkansas.

Arming intelligence with Web 2.0

By Michael Wertheimer
Assistant Deputy Director
Office of the Director
of National Intelligence, U.S.

It is easy to forget that the World Wide Web is just a teenager. In fact, it was a mere 15 years ago that the first web browser was introduced to the Internet. Today, 1.4 billion online users log onto the web each day — a revolution by any standard.

Many experts agree that the Internet is now in its second generation — a generation often referred to as Web 2.0. This second wave of the Internet relies more on users contributing to content, and is driving the Internet to a social network.

But Web 2.0 has also created new venues for illicit activities. From crime to terrorism, the Information Age delivers fearsome capabilities to those who would seek to do harm. Web 2.0 offers enticing opportunities to exploit technology for good or for ill. Understanding how these technologies can be used by adversaries is a significant challenge — a challenge that the United States Intelligence Community (IC) is pursuing with vigour.

The new intelligence environment

The IC consists of 16 federal agencies, offices and elements of organizations that are collectively responsible for gathering, analyzing and disseminating intelligence information in the United States. Like the law enforcement community, the IC recognizes that "business as usual" no longer applies in the current Web 2.0 environment.

Mike McConnell, U.S. Director of National Intelligence and head of the IC, describes web-savvy adversaries as follows: "These new actors blur the traditional distinctions between foreign and domestic, intelligence-related and operational, strategic and tactical."

How the IC operates in this context — today and for every day after — is critically important and requires creative problem solving, particularly given a number of other nettlesome challenges:

- A very young analytic workforce, 60 per cent of whom were hired after 9/11
- Diverse and voluminous data that tends to overwhelm analysts
- Aging information technology systems that cannot support sophisticated tools
- Traditional analytic techniques, perfected for the world of nation-states, that founder in the face of non-state actors
- An increasing tendency to subject analytic judgments to public exposure and scrutiny

The IC is beginning to address these challenges through exciting initiatives aimed at bringing the power of information-sharing and collaboration to intelligence analysis. Led by the Office of the Director of National Intelligence (ODNI), the IC is drawing on the lessons of Web 2.0 to create social networks, collaboratively generate knowledge, and empower a young and enthusiastic workforce.

"ODNI is pulling the levers of power to reform our intelligence community," says Dr. Donald Kerr, principal deputy director of national intelligence. "This isn't glamorous work. It isn't easily distinguishable to those outside the community, but more than anything else, this is the work that needs to get done."

Two projects exemplify the IC's future direction: Intellipedia and A-Space. While it is tempting to think of these as new tools, ODNI thinks of them more as game-changing initiatives — new ways to work and do business — that will radically broaden intelligence work.

A new way to wiki

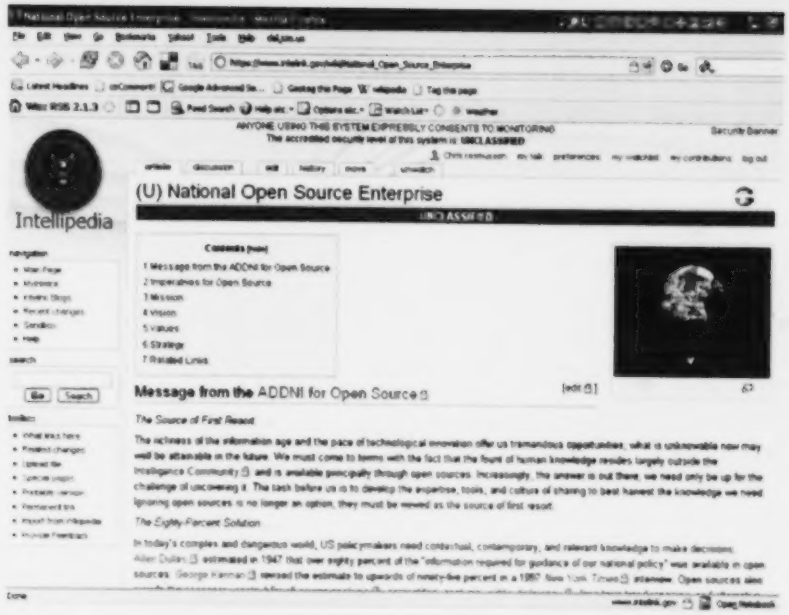
The seventh most popular site on the Internet is the online encyclopedia Wikipedia. Unlike conventional encyclopedias, Wikipedia is written entirely by volunteer contributors who freely edit and author articles as a collective, achieving accuracy rates that rival peer-reviewed, professionally edited products.

According to Dr. Thomas Fingar, the ODNI Deputy Director of Analysis, Wikipedia processes are "an absolutely innate approach" for the IC's younger workforce — the "digital generation" that simultaneously reads e-mail, talks on the phone, watches television, and has a conversation while linked with people around the world. But for the rest of the IC, says Fingar, the Wikipedia approach "is somewhere between heretical and previously deemed impossible."

In April 2006, the IC officially launched Intellipedia, its own collaborative system to connect analysts, working groups, collectors, experts, data and knowledge. Like Wikipedia, Intellipedia enables users to post, edit and enhance articles. Unlike Wikipedia, all contributors are accountable — there is no anonymity. Furthermore, Intellipedia operates at three classification levels, permitting users from across the IC and law enforcement communities to access and contribute to it.

Creating Intellipedia was easy because it uses MediaWiki — the same software used by Wikipedia — which is freely available. The cost was very low and remains so. The resistance was not particularly strong because Intellipedia was a new capability and threatened no existing processes.

Two years after launch, Intellipedia holds more than 330,000 pages and boasts 42,204 registered users (who cross all demographics) and approximately 135,000 readers. The growth has been nothing short of spectacular. Intellipedia reached the million-edit mark two


ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO MONITORING
(U) National Open Source Enterprise
Intellipedia
Message from the ADDNI for Open Source
The Source of First Resort
The Eighty-Percent Solution

Two years after launch, Intellipedia holds more than 330,000 pages and boasts 42,204 registered users and approximately 135,000 readers.

months earlier than it took Wikipedia to reach the same point.

But Intellipedia is more than a repository of information — it is evolving into a tool that enables intelligence officers around the world to analyze crises as they unfold. At a time when CNN fills the airwaves with fast-breaking news and citizens watch scrolling news feeds at the bottom of their computer screens, Intellipedia is emerging as a powerful tool to share information and analyze global incidents in near-real time.

Political officers at an overseas embassy can easily post breaking news, alerting geospatial intelligence analysts, who then share updated maps with layers of information, and military analysts, who examine and report troop levels and capabilities. Analysts from across the IC are starting to use Intellipedia to fuse their analyses instead of publishing myriad independent reports from their home agencies.

For example, in 2006, a small two-seater plane crashed into a Manhattan building. Was it a terrorist incident or an accident? Within 20 minutes of the crash, an analyst created an Intellipedia page, which was edited 80 times in the next two hours by members of nine different intelligence agencies. They collaborated and rapidly concluded that the collision was an accident. The speed, thoroughness and multi-disciplinary nature of the analysis were unprecedented.

The next big idea

Intelligence analysts demand a working environment that gives them unfettered access to the best expertise — regardless of where it resides — and allows them to investigate, discover and explore new ways to perform analysis. Building on the momentum created by Intellipedia, ODNI is piloting a tool called A-Space (Analysis Space) that will meet these needs.

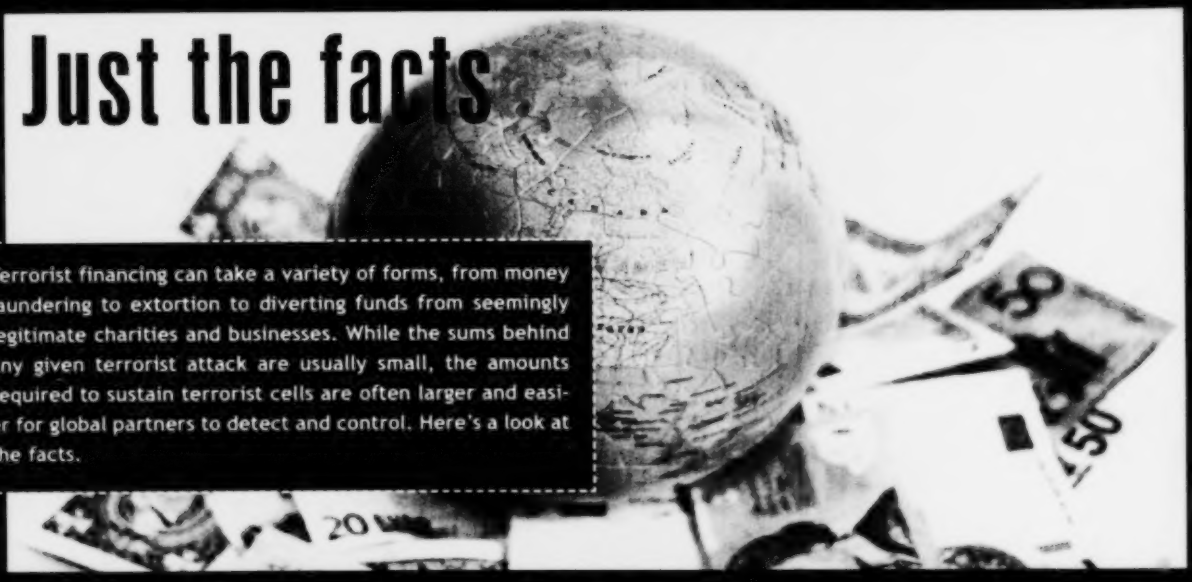
Set for launch this fall, A-Space complements Intellipedia and takes another step towards a true World Wide Web for analysts by providing them with a new environment in which to work. For the first time, analysts will have common access to documents and information several levels above top secret — including databases residing in agencies other than their own. Because A-Space rigorously enforces its entrance requirements to include specific security clearances, it will become a trusted environment for all IC analysts.

A-Space will also provide the shortest, fastest path to discovering IC expertise and emerging intelligence insights, allowing analysts to collaborate early and often. Some have likened A-Space to Facebook for the IC. While A-Space does have a social networking function that allows analysts to post profiles detailing their areas of past and current expertise, it is much more than that.

For example, IC analysts are notorious for organizing their notes on their individual computer desktops, making it difficult to share insights with others. With A-Space, analysts will be able to share their personal "file folders" through a secure "file cabinet." They can create common work spaces supported by instant messaging, shared documents, and RSS feeds. The IC will be able to virtually "swarm" to tackle intelligence questions.

As time passes, IC analysts will discover and invent previously unimaginable uses for Intellipedia and A-Space, ultimately shaping the future of the intelligence business. Intellipedia and A-Space are precursors for the day when Web 2.0 denizens will find themselves stunned by the intelligence community's agility, imagination and effectiveness on the World Wide Web. ■

Just the facts



Terrorist financing can take a variety of forms, from money laundering to extortion to diverting funds from seemingly legitimate charities and businesses. While the sums behind any given terrorist attack are usually small, the amounts required to sustain terrorist cells are often larger and easier for global partners to detect and control. Here's a look at the facts.

Terrorists spent an estimated £8,000 to carry out the London transit bombings in July 2005.

Of the US$400,000–500,000 required to carry out the 9/11 attacks, $300,000 passed through the U.S. banking system, according to research by the National Commission on Terrorist Attacks Upon the United States.

The sums that circulated between the 9/11 hijackers and their overseas accounts amounted to less than US$10,000 and were often simple wire transfers, reports the International Monetary Fund.

Prior to 9/11, al-Qaida spent an estimated US$30 million per year to fund operations, maintain training and military apparatus, and contribute to the Taliban and related terrorist organizations, according to the National Commission on Terrorist Attacks.

One terrorist group operating prior to 2001 collected up to US$1 million per month from expatriates in Canada, Britain, Switzerland and Australia, reports the Financial Action Task Force (FATF).

The FATF points to the misuse of non-profit organizations as "a crucial weak point" in the global struggle to stop terrorist funding at its source.

In 2006–2007, Canada's Financial Transactions and Reports Analysis Centre (FINTRAC) reported 33 cases of suspected terrorist financing or other threats to Canadian security, representing a total value of C$200 million.

Eight additional FINTRAC disclosures involving both terrorist financing and money laundering totalled C$1.6 billion.

In 2007, American depository institutions submitted 25 per cent less suspicious incident reports related to terrorist financing than they did in 2004, according to U.S. Treasury numbers.

As of August 19, 2005, the U.S. had frozen or blocked over US$281 million in property assets linked to 303 suspected terrorists or terrorist entities, as per United Nations resolutions.

As of 2007, the U.K. had frozen nearly 200 bank accounts and half a million pounds linked to designated terrorist suspects.

Between September 2001 and July 2007, the U.S. Department of Justice convicted 59 individuals of crimes related to terrorist financing. Canada laid its first charges in March 2008.

SOURCES: Financial Action Task Force (FATF), "Terrorist Financing Typologies Report" (29 February 2008); "Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: United States of America" (23 June 2006) : **www.fatf-gafi.org** ; National Commission on Terrorist Attacks Upon the United States, "Monograph on Terrorist Financing" : **govinfo.library.unt.edu/911/staff_statements/index.htm** ; International Monetary Fund, "The Impact of Terrorism on Financial Markets" (March 2005) : **www.imf.org/external/np/leg/amlcft/eng/** ; Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), "FINTRAC Annual Report 2007" : **www.fintrac-canafe.gc.ca/publications/ar/2007/41-eng.asp** ; United States Department of the Treasury, Financial Crimes Enforcement Network, "SAR Activity Review - By the Numbers - Issue 9 (February 2008)" : **www.fincen.gov/pub_reports.html** ; Her Majesty's Treasury, "The Financial Challenge to Crime and Terrorism" (February 2007): **www.hm-treasury.gov.uk/documents/financial_services/money/fin_money_financialchallenge.cfm** ; The Investigative Project on Terrorism, "Finally, some sanity (and accuracy) in assessing DOJ terrorist financing efforts" (16 February 2008) : **www.investigativeproject.org/article/608** ; The Globe and Mail, "CSIS looks for new means to track terrorist financing" (21 April 2008): **www.theglobeandmail.com**

Canadian experts assist with Guatemalan bus crash investigation

By Cal Deedman
Crown Counsel
Ministry of the Attorney General
of British Columbia (B.C.)

Travel in Guatemala on the so-called "chicken buses" is a hazardous business. Most of the buses are overcrowded, overloaded, poorly maintained and recklessly driven. Stories of crashes in which people have been killed or injured appear in the local press with depressing regularity, yet they rarely make the international media.

Guatemalans tend to accept these bus accidents as an unavoidable part of daily life. However, on Feb. 29, 2008, there was a bus crash with such horrendous consequences that it attracted international media coverage, shocked the Guatemalans themselves and prompted a national outcry for a full investigation.

The bus, travelling along the highway leading to El Salvador, failed to negotiate a right-hand curve 33.5 kilometres east of Guatemala City, just short of the bottom of a long downgrade. It veered across the oncoming lanes, went off the road, plunged through a small gully, and slammed head-on into a dirt embankment. Fifty-six passengers died as a result of the accident, and people demanded to know why.

Lacking the resources and expertise to do such an investigation themselves, the Guatemalan government turned to Canada for help.

In Guatemala, the Public Prosecutor's Office (called the Public Ministry) is responsible for directing investigations into suspected crimes.

The Public Ministry sent a formal request for assistance to Kenneth M. Cook, the Canadian Ambassador to Guatemala. The embassy's political counsellor passed the request to S/Sgt Vianney Tremblay, the RCMP Liaison Officer for Mexico and Central America. With the help of RCMP National Traffic Services and the National Program Manager for Collision/Analyst Reconstruction, S/Sgt Tremblay assembled a team of Canadian experts and arranged for them to travel to Guatemala.

The three-man team was composed of Sgt Larry Bellows and Cpl Peter Holmes, two collision reconstructionists, and Robert Richardson, a mechanical inspector with the B.C. Ministry of Transportation.

The team flew to Guatemala and met with the local prosecutors for a detailed review of the file.

They also appeared before the judge responsible for overseeing the investigation and were granted official legal status as experts. This entitled them to investigate the accident and to give evidence about their conclusions. They would testify at a special hearing held before they returned to Canada.

The team attended the scene of the crash to take measurements and photographs, and to analyze the overall context in which the accident had happened in an attempt to determine its causes. They also visited the compound where the remains of the bus were stored and conducted a mechanical inspection.

The team then spent six days going over their findings, preparing their collision reconstruction and mechanical inspection reports, and arranging to have the reports translated into Spanish for the hearing.

Conclusions

The Canadian experts' conclusions were damning. The rear brakes of the bus were completely non-functional at the time of the accident, and the front brakes were in poor condition. Although the front brakes initially provided a 30 per cent braking capacity, they overheated and eventually faded after being steadily applied for approximately 14 kilometres on the continuous seven per cent downgrade. By the time the bus reached what is known as the *El Chilero* curve, about two kilometres from the bottom of the slope, the brakes failed.

Cpl Peter Holmes

Sgt Larry Bellows and Robert Richardson conduct a mechanical inspection of the Guatemalan bus. The Canadian experts found numerous defects due to heavy use and poor maintenance.

The bus also had a series of other defects contributing to its overall instability: the steering mechanism was loose, the suspension was badly worn and different-sized tires were installed on the same axle.

Finally, although the bus had a maximum seating capacity of 48, it was carrying 82 passengers at the time of the accident.

It seems certain that there will be criminal and civil proceedings arising out of this accident and that the evidence provided by the Canadian experts will play a key role in those proceedings. ■

Since 2001, the RCMP, in partnership with the B.C. Ministry of the Attorney General and the Law Courts Education Society of B.C., has been working with the Guatemalan Public Ministry and National Civil Police, training prosecutors and investigators in crime scene examination, major crime investigative techniques and major case management.

Managing police fatigue: a high-wire act

By Bryan Vila, PhD
Washington State University

Anyone who's ever been to the circus knows what a complex balancing act is required of the daring acrobats who walk the high wire. While some attempt the feat "free-handed," most use some sort of prop, such as a long drooping pole, to help maintain their balance as they walk the fine line between two points.

Managing police fatigue is an equally complex balancing act that involves the needs of the community, the department, and the officers themselves. Most police departments today still attempt to address this issue "free-handed." But a growing number are beginning to work closely with sleep researchers who can provide them with the props they need — in the form of recommendations and tools based on recent scientific studies — to make the task much easier.

This article addresses just a few of the ways these studies can help improve staffing decisions, shift scheduling, overtime management and other issues that affect officers' sleep, and ultimately their health, safety and job performance.

Balancing needs

Policing is one of the most critical and expensive government activities. It is essential that communities have sufficient officers on duty at any given time to respond to emergencies, prevent crime and arrest offenders. It is equally important that public resources are not wasted by having too many officers on duty. To complicate matters, every community generates a unique demand for police services that tends to rise and fall across the day, week and season.

The problem of scheduling just enough officers is compounded by the complexities of managing fatigue. If officers are impaired by fatigue, they become less alert, their cognitive and physical abilities decline, their moods worsen and they become less able to deal with stress. Public safety declines — and so does officer safety and performance, resulting in a higher risk of job-related accidents, injuries, errors and misconduct.

Over the long term, fatigue makes officers more vulnerable to illness, chronic disorders and certain kinds of cancers. Fatigue also corrodes the quality of an officer's family life. It is therefore in everyone's best interest to understand the causes of police fatigue and to learn how best to manage and mitigate those causes.

Fatigue makes officers more vulnerable to illness, chronic disorders and certain kinds of cancers. It in everyone's best interest to understand the causes of police fatigue and to learn how best to manage and mitigate those causes.

Causes of police fatigue

In shift workers such as police officers, fatigue and its effects are rooted in four different variables.

Time of day — Police work is a 24/7 activity, but the biochemical, physiological and behavioural systems of human bodies are synchronized by circadian rhythms that strongly favour working during the day and sleeping at night. Police officers, like all humans, tend to be much more vulnerable to fatigue from 11 p.m. to 6 a.m.

Quantity of sleep — Our sleep reservoirs fill up when we sleep for 7.5 to eight hours, and then are drained during each waking hour. This means an officer who gets a full quota of sleep, rises at 7 a.m., then starts a 12-hour shift at 11 a.m. is likely to be very impaired by 11 p.m. — roughly the equivalent of a blood alcohol concentration of .05 per cent. If the officer starts her shift with less than a full quota of sleep, she is likely to be even more impaired by the end of her shift. Moreover, sleep debt is cumulative and, if not repaid, will likely cause the officer to become increasingly impaired over time.

Quality of sleep — Many police officers have serious sleep disorders that disrupt sleep or make it difficult to fall asleep and stay asleep. A sleep-disordered officer who spends eight hours in bed each night (or day) may not be getting enough quality sleep to make it through a work shift safely. Currently, the only way to manage this problem is to have officers screened periodically by a qualified sleep physician.

Number of sequential work days — Police officers, like all people, get progressively more tired with each day of work. This effect is especially pronounced if the successive shifts require officers to sleep during the day rather than during the night, since night sleep is much more natural and tends to be more restorative. While many people try to catch up on lost sleep during their days off, this may be impossible for an officer whose sleep debt is too large to be repaid.

Managing and mitigating fatigue

Managing and mitigating fatigue requires striking a balance between police officers' circadian rhythms and the rhythms of society. But in addition to balancing a community's demand for services against officers' physiological needs, managers must also find ways to mitigate the impact of scheduling on officers' lives outside the job.

The success of any fatigue-management effort requires officers to practise good sleep habits. It takes training in sleep practices and real commitment for an officer to get sufficient sleep during the day when noise, light and circadian rhythms are fighting to keep him awake. Moreover, since the majority of society is organized to be active during the day and evening, a day-sleeper's world is full of temptations to

be with loved ones, attend to errands or get in a round of golf.

Shift schedules must be as stable as possible in order to encourage good sleep practices and minimize stress on officers. Erratic work hours make shift work even more difficult because they interfere with nearly every aspect of life, breaking routines and increasing problems associated with everything from picking up the kids from school to planning an evening with friends.

The main cause of erratic work hours for most police officers is overtime caused by late arrests, off-duty court appearances, emergencies, or the need to increase staff for public events. Another cause is moonlighting (secondary employment). The best way to minimize inconsistent work hours is to ensure that staffing numbers match the demand for police services — and to drastically limit moonlighting.

Creating change

Despite the obvious importance of managing fatigue, most police agencies have a hard time with this issue, largely because of the allure of overtime. Even though overtime is a convenient way for managers to patch gaps between demand and available staff — and for officers to earn more money — it must be minimized. In my experience, the best fatigue management practices grow out of a close collaboration between management and labour that is informed by hard science.

Science provides a common ground where hard evidence helps balance conditions-of-work negotiations. It forces managers to confront the real risks and costs of fatigue, and it forces officers and their representatives to focus on their first priorities: safety and health. Both sides have to cooperate. Risks and costs can't be controlled unless officers make sleep a priority and come to work rested. But they cannot do so unless work hours, schedules and staffing are appropriate. Co-operation is the only way either side can get what it needs.

However, good intentions alone can't solve a very complex scheduling problem and reconcile that solution with the immutable biological demands of officers' circadian rhythms. This problem requires substantial mathematical skills and a deep understanding of human sleep.

The Calgary Police Service (CPS) is taking an exemplary approach to this problem by involving a skilled operations researcher, Peter Belmio, to help analyze the demand for services and develop scheduling options. They're working with a sleep researcher — Dr. Charles Samuels of the University of Calgary's Centre for Sleep and Human Performance — who is developing techniques for measuring the impact of different schedules on officers' alertness and cognitive performance. CPS has also worked with me to begin educating officers and supervisors about sleep issues and strategies for maintaining good sleep habits.

This collaborative effort strives to identify problems and acquire hard evidence that will make it possible to build shift schedules that balance the needs of Calgary's communities with those of its officers. But there is still much to do. Future plans include finding ways to integrate evidence-based scheduling and work-hours management into CPS policies and practices — such as by refining shift work and sleep education programs for officers and their families, and by developing health screening systems that are economical, practical and scientifically rigorous.

The hands-on work of police agencies such as CPS is part of an even larger collaborative effort by research teams at Washington State University, the U.S. National Institute for Occupational Health and Safety, the State University of New York at Buffalo, Harvard University and the University of California, San Francisco. The goal is to build knowledge and tools that can help police everywhere balance the needs of communities with those of the officers who serve them. ■

Bryan Vila, PhD, is a professor of criminal justice at Washington State University and a senior investigator in its Sleep and Performance Research Center. Vila served as a law enforcement officer for 17 years. He has authored numerous research articles and three books, including Tired Cops: The Importance of Managing Police Fatigue *(Police Executive Research Forum, 2000).*

Body-worn video

The pros and cons of using head cameras

Optical evidence-gathering has been used by police since the advent of the camera and has continued to improve with technological advancement. In 2005, Sgt Olly Tayler of the Devon and Cornwall Constabulary in the southwest of England proposed the use of a new concept in evidence gathering called body-worn video (BWV). In this article, Tayler outlines the strengths and weaknesses of BWV based on the pilot project he managed in Plymouth, U.K.

By Sgt Olly Tayler
Devon and Cornwall Constabulary (U.K.)
Plymouth Head Camera Project

Body-worn video (BWV), also known as a head camera, consists of a lipstick-sized full-colour bullet camera attached to a small digital hard drive unit. High-quality digital footage and audio can be stored on the unit and later downloaded to computer or burned to disc.

The camera is worn on the side of an officer's head or uniform headwear by way of an adjustable headband. Officers also carry the digital hard drive unit that contains a rechargeable battery. A remote switch allows the officer to start and stop recording, while a visible light indicator enables others to see when the camera is recording or in standby mode. The video and audio data provide an officer's view of how an incident unfolded, who said what, and what decisions were made at the time. The camera also captures emotions and many small details that can be forgotten during the dynamics of an incident.

Police officers involved in the Plymouth Head Camera Project reported that the device had a calming influence on potentially violent people.

Courtesy of the Hampshire Constabulary

Most BWV systems have built-in LCD screens that permit officers to review footage on the street. This feature is valuable during public disorder incidents, as it allows officers to review footage on site to ensure they have the best possible chance of identifying victims, suspects and potential witnesses.

BWV pilot project

Devon and Cornwall police participated in a small proof-of-concept BWV pilot in the City of Plymouth. Known as the Plymouth Head Camera Project, the pilot ran from October 2006 to March 2007. It concentrated on providing head cameras to officers attending violence-related calls, including those involving alcohol-related violence, violence in public places and domestic violence.

Police purchased 50 sets of BWV and trained nearly 400 front-line officers to use them. Officers were given guidance on when to start and stop recording — typically as soon as a call is received though to its natural conclusion. Officers were also given discretion to record at other times when they felt it would be of value, such as at a traffic stop. They avoided turning the system off mid-recording without a verbal explanation as to why.

The Constabulary also undertook an extensive internal and external media campaign using television and newspaper announcements and targeted posters to ensure that police officers, other police staff, the general public, and at-risk groups were fully engaged in the concept.

Following the pilot, a full and independent project evaluation concluded that using BWV resulted in a reduction in crime, an increase in crimes detected, an increase in offenders brought to justice, a reduction in complaints against officers, and an increase in public confidence in policing.

As well as the formal evaluation, officers involved in the Plymouth pilot provided considerable anecdotal evidence that using head cameras had a noticeable calming influence on

potentially violent persons and resulted in better engagement between police and young people.

Officers also found new and innovative ways of using BWV beyond basic evidence gathering at incidents of violence. For example, officers used the device to help reconstruct a fatal road traffic collision, to obtain details and descriptions from young people at a party where a serious allegation had been made, and to view places that have traditionally been hard to access — such as under floor boards — during drug searches. Police tutors have also used BWV to record and debrief student police officers dealing with live incidents.

Advantages

The use of BWV can dramatically enhance the gathering of primary evidence at any incident. The camera can pick up and record everything an officer sees and hears, including details officers could never hope to recall when trying to document events on paper in a statement.

There have been countless examples of BWV being used to help secure convictions by ensuring offenders admit to their wrongdoings at much earlier stages in investigations.

BWV footage has also been used to disprove malicious complaints against police officers. There have been examples of solicitors making complaints on behalf of their clients then immediately withdrawing those complaints after reviewing BWV footage.

BWV evidence has been used in courts to show what happened at an incident. A prepared statement can come across as very clinical and does not convey the emotions and atmosphere at the time an officer interacted with an offender. Head cameras, however, can capture those emotions.

When used in domestic violence situations, early accounts from victims and evidence of injuries can be documented using BWV. In the event that a complaint is subsequently withdrawn, the case can still proceed as a victimless prosecution, thereby ensuring that offenders are held to account in court.

BWV footage can also be logged and sorted in a video intelligence database housed in a back-office facility. The database used for the pilot in Plymouth now contains tens of thousands of hours of footage, providing officers with access to images of suspects and the clothing they were wearing on a specific day, evidence of patterns of offending behaviour, and evidence to support applications such as anti-social behaviour orders. Images can be taken from the database and used in briefing papers or media appeals. Footage of buildings or other premises can be used to help officers plan for future warrants or, in the event of critical incidents, assist commanders with ground-level planning.

While BWV is a relatively new concept for police, it has proven itself to be a valuable tool for gathering primary evidence at any policing incident or event.

Limitations

An obvious disadvantage of BWV is that an officer has to be looking at an incident to capture the best evidence. Furthermore, when a single camera is deployed at an incident, it will only capture a single viewpoint. During many incidents of disorder, what is happening on the periphery can be as important as the main incident.

Another drawback is that, like any other technology, BWV can fail. While a number of safeguards are built into the technology to protect against this, there is still a chance of a complete system failure and the resulting loss of crucial footage. The deployment of BWV should not replace an officer's best optical and audio evidence-gathering equipment: his or her eyes and ears.

There are two principal technological limitations of BWV as it exists today: battery life, particularly in extreme weather conditions, and durability of the internal hard drives, since a mere knock or jolt can corrupt data as it is being written.

In the case of batteries, the technology is improving all the time and battery capacity has increased dramatically over recent months. Regarding durability, many BWV developers are now employing removable media such as Secure Digital (SD) cards to ensure that head cameras are suitable for the rigours of modern-day policing. Using removable media also means that a BWV unit can be processed and put back into service very quickly.

While the limitations may be seen as inhibitors to using BWV, the benefits speak for themselves and any evidence the camera captures is better than none.

Moving forward

The U.K. Home Office used the experiences and findings of the Plymouth pilot project as a national proof-of-concept for the U.K. Police Service (43 Home Office forces) and produced a manual called "Guidance for the police use of body-worn video devices."

Since the completion of the pilot, the majority of U.K. police forces have purchased and are using the device. There has also been extensive interest from other countries; a number of equipment trials are currently being undertaken in Singapore, South Africa and China. The concept of BWV is also being assessed by the wider U.K. security industry including the Customs Service, the Border Agency and the Ministry of Defence.

Conclusion

While BWV is a relatively new concept for police, it has proven itself to be a valuable tool for gathering primary evidence at any policing incident or event. The technology is being improved all the time, and the next generation of BWV may include wireless systems and built-in automatic-license-plate-recognition (ALPR) and biometric-recognition software. Future links between BWV and intelligent PDAs may further reduce the paperwork burden on officers while improving performance across the justice system. ■

Latest research in law enforcement

The following are excerpts from recent research related to justice and law enforcement. To access the full reports, please visit the website links at the bottom of each summary.

Predictive factors for illicit drug use among young people

By Martin Frisher et al.
For the Research Development and Statistics Directorate, Home Office (U.K.)

This report presents the results of a literature review on predictive factors for drug use among young people. A systematic search of electronic databases identified 251 relevant papers of adequate quality. Of these, 78 were randomly selected for further analysis.

The most extensive and consistent evidence relates to young people's interaction with their families. The key predictors of drug use are parental discipline, family cohesion and parental monitoring. Some aspects of family structure such as large family size and low parental age are linked to adolescent drug use.

There is also consistent evidence linking peer drug use and drug availability to adolescent drug use. There is extensive evidence on parental substance use, although some studies report no association while others indicate that the association is attenuated by strong family cohesion.

Age is strongly associated with prevalence of drug use among young people, reflecting a range of factors including drug availability, peer relationships and reduced parental monitoring.

Categories where evidence linking specific factors is mixed include mental health, Attention Deficit Hyperactivity Disorder (ADHD), stimulant therapy, religious involvement, sport, health educator interventions, school performance, early onset of substance use and socioeconomic status.

The overall ratio of risk to protection may be more important than any individual factor. These results, although supported by a relatively small body of research, support the concept of resilience to drug use. According to this view, resilience to drug use is enhanced by increasing social skills, social attachments and material resources despite constant exposure to known risk factors.

"Age is strongly associated with prevalence of drug use among young people, reflecting a range of factors including drug availability, peer relationships and reduced parental monitoring."

Whereas risk and resilience are, to a large extent, independent of individuals' motives, there is evidence that the latter are just as important as the former in determining drug use. Young drug users consistently report getting intoxicated and relief from negative mood states as reasons for their drug use. Qualitative research shows that the context in which young people experience drugs is crucial for understanding how risk and protective factors operate in relation to experimental and sustained drug use.

Risk factors have differential predictive values throughout adolescence. Some factors may occur at birth (or before) while others occur at varying times throughout adolescence. Some factors may persist for long periods of time while others are transitory. The distinction between early and late onset risk factors is important as preventive measures need to focus on particular age groups.

To access the full report (RDS OLR 05/07), please visit: ***www.homeoffice.gov.uk/rds/onlinepubs1.html***

Snitches get stitches: youth, gangs and witness intimidation in Massachusetts

By Julie L. Whitman, MSW, and Robert C. Davis, MS
For the National Centre for Victims of Crime (U.S.)

It is a familiar story: a gun goes off in a crowded place — perhaps a street festival or a nightclub — someone ends up dead, and when police officers begin questioning the bystanders, "nobody saw anything." Officers charged with investigating such crimes and apprehending the offenders know only too well the chilling effect of witness intimidation on the criminal justice process.

The National Centre for Victims of Crime conducted this study to better understand the intimidation of teen and young adult witnesses in gang-related cases. This first-of-its-kind investigation gathered information directly from youth about (a) the critical factors that deter youth witnesses from reporting gang crimes and testifying against perpetrators, and (b) the kinds of policies and programs that can encourage victim and witness co-operation.

Key findings (partial list):

- Youth had a high rate of exposure to crimes through direct victimization, witnessing, and peer and family victimization.
- Youth are most likely to tell a parent or other family member about experiences with crime.
- Community norms against "snitching" are strong, but youth

> **"When it comes to reporting crime and participating in the criminal justice process, the youth were clear: if they felt an officer was trustworthy and respectful, they had no problems talking with that officer."**

were still willing to report crimes under certain circumstances.
- Vicarious experiences of witness intimidation were far more common than personal experiences, but one in three youth had heard about someone being threatened.
- Relationships between youth and school resource officers were generally positive; relationships with neighborhood police officers were mixed.

Recommendations

The study findings indicate at least six areas where local criminal justice authorities and community groups can focus to improve the participation in the criminal justice process of young witnesses to gang crimes. More information on these recommendations can be found in the full report.

Implications for police and prosecutors

One of the clearest messages from the youth in the study was a plea for better police community relations. When it comes to reporting crime and participating in the criminal justice process, the youth were clear: if they felt an officer was trustworthy and respectful, they had no problems talking with that officer.

Another step police can take to make crime reporting safer is to be extremely careful not to identify witnesses unnecessarily. A certain amount of anonymity or confidentiality should be possible in the early stages of investigating crimes.

When vulnerable witnesses are involved, criminal justice officials must either establish a single point of contact in the system for the witness or ensure a seamless transition of witness communications from police to prosecutor to victim/witness co-ordinator.

The criminal justice response to witness fears and reported attempts at intimidation can and should vary according to the details of the case. Local prosecutors and police officers should develop a varied collection of witness protection measures they can employ as needs arise.

To access the full report (including the "law enforcement" research summary from which this excerpt is drawn), please visit: ***www.ncvc.org/reports***

Integrated intelligence and crime analysis

By Jerry H. Ratcliffe, PhD
For the United States Department of Justice

Law enforcement executives are increasingly recognizing that they are no longer in an information-poor world: data and information about the criminal environment and criminal activity abound.

In many cases, however, this increase in data has not necessarily translated to an increase in knowledge. The structure of information handling processes within policing is not set up for the new millennium and ideas about intelligence management and dissemination from the 1970s still pervade the thinking and organizational culture of police agencies in the 21st century. While many executives get access to crime analysis, criminal intelligence is not integrated into the picture and executives make key decisions without access to all of the pertinent knowledge available within their organization.

The purpose of this report is to provide the necessary information for police managers to implement change and embrace the information-rich environment of modern policing. The document is also of value to intelligence analysts and crime analysts wishing to get greater traction from the intelligence they produce.

This report starts by describing the differing roles that criminal intelligence and crime analysis play in the modern law enforcement environment. It then clarifies why the current situation — a separation of key functions, as commonly seen in many police departments — is both a hindrance to good policing in an intelligence-led policing environment and a risk to the communities that police are sworn to protect.

This report argues for an integrated analysis model that combines the functions of crime analysis and criminal intelligence and seeks to avoid analytical processes that separate information on offenders from information on the crimes that they commit. In support of this argument, this report identifies a range of ways that the integrated model can help decision makers and includes a number of examples to demonstrate this approach.

However, the hindrances to the development of this model are not insignificant. For example, problems discussed in this report include the following: issues of civilianization; differing missions and terminology between crime analysts and criminal intelligence officers; isolationist and case-specific thinking instead of concentrating on the big picture; perceived legal restraints on intelligence analysts; and a lack of training and education.

Finally, the report contains a number of practical recommendations for police departments wishing to better integrate these necessary functions (crime analysis and criminal intelligence) and become more intelligence-led and problem-focused.

To access the full report, please visit: ***www.cops.usdoj.gov/ric/ResourceDetail.aspx?RID=433***

Alberta initiative targets domestic violence

By Valerie J. Campbell
Director, ARTAMI

According to Brian Vallee, author of The War on Women, between 2000 and 2006, more than 500 Canadian women were shot, stabbed, strangled or beaten to death by their intimate male partners — five times more than all of the Canadian soldiers and police officers killed in the line of duty during that same time period.

In Alberta and jurisdictions throughout Canada, homicides have continued to occur between intimate and ex-intimate partners, and sometimes their children and other family members. Often, victims of family violence fatalities were in contact with multiple professional and community-level support services prior to their deaths, yet they managed to fall through the cracks. When one of these tragedies occurs, it serves as a reminder of why family violence needs to be taken seriously and how much more work still needs to be done to address the complexities of preventing these deaths.

There is a growing recognition that many family violence-related deaths are preventable. In a number of fatality cases reviewed by the Ontario Domestic Violence Death Review Committee (DVDRC) in 2005, the perpetrator had previously been recognized as dangerous and the victim had been identified as being at high risk. Unfortunately, there was no effective case management response, resulting in dire consequences for the victim. According to the DVDRC, many of the fatalities reviewed appeared to be predictable and preventable, with the benefit of hindsight and the analysis of well-known risk factors.

Domestic violence is not only one of the highest calls for police response, but perhaps the most frustrating and difficult to understand, particularly from a criminal justice perspective. Fearful and reluctant victims, patterns of abuse that continue (in some cases) for years, and child custody and access disputes are the most common factors that inhibit protection for victims and plague well-intentioned police investigations.

Whether you are a police member in a remote two-person detachment or part of a specialized unit in a large municipal police agency, the issues are the same. How can you protect a victim who is unwilling or unable to co-operate? How do you know when a particular case is high risk and may result in murder or murder/suicide? What can you do to prevent these kinds of tragedies from occurring even if you could predict them?

Reducing the risk

Answers to these questions are more available than one might think. In 2007, the Alberta government created a specialized unit to do just that. The Alberta Relationship Threat Assessment and Management Initiative (ARTAMI) became the first threat assessment unit in Canada to involve experts from various fields and multiple law enforcement agencies who deal solely with high-risk relationship violence and stalking cases.

ARTAMI was created after the victim of one of the longest and most extreme stalking cases in Canada made a plea for a better approach to threat assessment in Alberta. A diverse committee including government, police and community agencies spent three years developing the initiative.

ARTAMI consists of police members from the RCMP and the Calgary, Edmonton, Medicine Hat and Lethbridge police services, teamed up with a Crown prosecutor, a child protection expert, a family law expert and a consulting psychologist. Police officers specially trained in threat analysis provide police and criminal justice agencies across Alberta with the following services:

- Formal threat assessments and case management plans
- Recommendations in respect of investigations, charges, court orders, victim safety requirements and strategies
- Expert court testimony for purposes of bail and sentencing hearings, child custody and access hearings, and guardianship applications
- Participation in case conferencing
- Specialized training in domestic violence, stalking and assessment and management of high-risk cases

ARTAMI's mandate is to identify individuals who pose a risk to others within the

ARTAMI's objectives

- Reduce the number of relational violent situations that result in serious violence, including homicide and/or suicide
- Integrate the criminal justice response to stalking and stop criminal harassment, as well as other acts of relationship violence
- Develop expertise within ARTAMI and utilize its professionals to enhance existing assessment programs for high-risk cases from a multi-disciplinary perspective
- Consult on long-term and dangerous offender applications for offenders who have extensive histories of relationship-related violence
- Collaborate with community agencies that assist victims of relational violence and their children to develop safety strategies
- Increase awareness of ARTAMI so community-based service providers know where to look for help when threats and violence in family relationships exceed the capacity of the local police services and other community agencies
- Maintain connections with diverse community agencies so ARTAMI can meet needs related to disability, language, culture, immigration status, sexual orientation, and/or street involvement

community and find the best way to manage and reduce the risk that the individual poses. All referrals to ARTAMI come through police services or prosecutors. Other outside agencies and actors — such as women's shelters, child intervention caseworkers and mental health professionals — may refer clients through their local police services.

Upon receiving a request from police, ARTAMI members review all of the material provided and, based on this review, identify risk and provide case management suggestions in the form of a written report. They also recommend victim safety planning or assist investigators in arranging to have a safety plan completed by another agency, such as a police-based victim services unit or the Alberta Child and Family Services authority.

By identifying the risk an individual may pose, investigators are better equipped to prioritize their cases in areas such as case management, officer safety and deployment of staff. Threat assessments categorize individuals to be at a low, moderate or high risk to commit an act of violence. A "low" categorization of risk does not imply "no risk," but indicates that the individual is at low risk to become violent and that the matter may continue to be monitored. "Moderate" risk indicates that the individual is at an elevated risk for violence and that any security measures in place should remain in place unless further measures are required. "High" risk indicates that the individual is at high or imminent risk for violence and that immediate intervention is required to prevent an act of violence from occurring.

Domestic violence is not only one of the highest calls for police response, but perhaps the most frustrating and difficult to understand.

Providing a detailed and accurate assessment of an individual's risk depends on the accuracy and thoroughness of the information used. As such, the more information that is available to investigators, the better. At minimum, this information should attempt to address or identify an individual's history in the areas of relationship, employment, childhood upbringing, mental health, substance use, weapon access, support networks and any other information investigators feel may assist the ARTAMI members. This information can be obtained from a number of records including police reports, mental health and medical reports, probation reports, witness statements and Correctional Service of Canada records. Where available, they should be provided to the ARTAMI investigator.

To ensure the objectivity and integrity of the threat assessment process, ARTAMI is not a first response unit and does not respond to crisis situations or crime scenes. Nor does it conduct or manage primary investigations or meet with offenders or witnesses.

Conclusion

In less than one full year of operation, ARTAMI has provided assistance in over 115 cases deemed to be high risk. Our goal is to reduce the fear, suffering and deaths that occur in high-risk cases by providing expertise in threat assessment and risk reduction.

Results from the Ontario Provincial Police Threat Assessment Unit (TAU) — a similar police-only initiative — demonstrate that intervention efforts can make a real difference in preventing family violence fatalities. In the 14 years that the TAU has been in operation, there has not been a single family violence-related fatality where the TAU was involved.

It is our hope that in the future, there will be no family violence-related fatalities in Alberta, particularly in cases where ARTAMI was involved. ■

Vancouver Police step into virtual reality

Courtesy of the Vancouver Police Department

The Vancouver Police Department was the first police service in the world to join Second Life.

Det/Cst Cherie Duggan
Vancouver Police Department

Like many large organizations, the Vancouver Police Department (VPD) has fallen casualty to the booming economy and the abundance of jobs. Attracting qualified applicants to join the police force is a constant challenge.

In 2003, the VPD received a total of 1,138 applications for the position of police constable. By 2006, that number had dwindled to 297. It became increasingly evident that the VPD Recruiting Unit would have to dramatically rethink how to recruit competitive applicants while still maintaining the essential requirements to apply. What the Department needed was an innovative and progressive way to boost recruitment.

Enter a group of forward-thinking individuals from the Masters of Digital Media (MDM) Program at the Great Northern Way Campus in Vancouver, B.C. Dr. Gerri Sinclair, the program's director, needed a novel way to attract the right mix of students for that program — students from the Flickr/YouTube/MySpace/Facebook generation.

In November 2006, after building a virtual copy of the school in Second Life — the most popular alternative universe on the web — Sinclair and her assistants held a recruiting day at both the real-world and Second-Life campuses. Insp Kevin McQuiggin of the VPD Forensic Services Section heard about MDM's Second Life initiative and felt that a similar approach might just be the key to reaching a new generation of police applicants.

Second Life, or SL, is an Internet-based virtual world that provides users with a venue to interact with each other through motional avatars (digital animated characters) and a social network service within the context of a metaverse (virtual world).

McQuiggin approached Sinclair about striking a partnership between the VPD and MDM, with the goal of holding a VPD information session in Second Life to attract potential recruits.

MDM agreed, offering the use of its virtual campus to host the online session and assisting first-time VPD users with SL navigation. Det/Cst Cherie Duggan of the VPD Recruiting Unit then collaborated with MDM to re-create the VPD's monthly real-world police information session for a virtual audience on Second Life. The objective was twofold: use the untapped medium of the virtual world to send the message that the VPD was hiring, and demonstrate the Department's progressive outlook.

On May 30, 2007, the VPD Recruiting Unit launched its Second Life Information Session. Duggan guided the online VPD avatar — dressed in a specially designed uniform complete with badge and utility belt — through a power point and video presentation, using the keyboard to communicate with other avatars. About 30 avatars turned out for the one-time online session, and four candidates e-mailed the Department with their resumés.

Was the online session a success? The answer is yes, from the perspective of drawing attention to a new recruiting option. The VPD was the first police department in the world to join Second Life. Although the SL session did not directly result in any new recruits, it did attract significant media coverage.

Most feedback has been positive and the interest generated from the initiative has been far-reaching. The story has been featured in the South China news, the Italian *Economy* magazine and the British *Police Professional* journal. Even a year after the launch, the VPD continues to receive e-mails from individuals who make reference to the Second Life Information Session. Most of the enquires have related to civilian Information Technology positions; however, one individual from Italy contacted and later met with a member of the VPD Recruiting Unit in Vancouver.

While the VPD's Second Life initiative did reach a large number of potential applicants, one drawback was the time required to design, create and maintain the site. It became too labour-intensive for one individual to continue indefinitely and required certain technical knowledge that many departments may not have nor wish to invest in.

That being said, the VPD would consider holding another Second Life session to attract job candidates as part of on-going recruiting drives. Today's tech-savvy online users have a skill set that is both transferrable to the world of policing and complementary to the other qualities that police departments seek in new recruits. ■